A Security Aware Fuzzy Enhanced ACO Routing Protocol in MANETs

Dissertation
zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
“Doctor rerum naturalium”
der Georg-August-Universität Göttingen

im Promotionsprogramm Computer Science (PCS)
der Georg-August University School of Science (GAUSS)

vorgelegt von

Hang Zhang
aus China

Göttingen, 2018

Betreuungsausschuss

Prof. Dr. Dieter Hogrefe,
Telematics Group, Institut für Informatik
Georg-August-Universität Göttingen

Prof. Dr. Xiaoming Fu,
Computer Networks Group, Institut für Informatik
Georg-August-Universität Göttingen

Dr. Parisa Memarmoshrefi,
Telematics Group, Institut für Informatik
Georg-August-Universität Göttingen

Mitglieder der Prüfungskommission

Referent:	Prof. Dr. Dieter Hogrefe, Telematics Group, Institut für Informatik, Georg-August-Universität Göttingen
Korreferent:	Prof. Dr. Xiaoming Fu, Computer Networks Group, Institut für Informatik, Georg-August-Universität Göttingen

Weitere Mitglieder der Prüfungskommission

Prof. Dr.-Ing. Marcus Baum,
Data Fusion Group, Institut für Informatik
Georg-August-Universität Göttingen

Prof. Dr. Carsten Damm,
Theoretical Computer Science Group, Institut für Informatik
Georg-August-Universität Göttingen

Prof. Dr. Delphine Reinhardt,
Computer Security and Privacy Group, Institut für Informatik
Georg-August-Universität Göttingen

Prof. Dr. Stephan Waack,
Theoretical Computer Science Group, Institut für Informatik,
Georg-August-Universität Göttingen

Tag der mündlichen Prüfung
10. October 2018

I hereby declare that I have written this thesis independently without any help from others and without the use of documents or aids other than those stated. I have mentioned all used sources and cited them correctly according to established academic citation rules.

Göttingen, September 2018

Acknowledgement

I owe tremendous thanks to many people I worked with during my studies. Without their recommendations and supports, this thesis would not have been possible.

I would like to give my deep gratitude and sincere appreciation to Prof. Dr. Dieter Hogrefe for his supervision. It was his constant guidance, support, and encouragement that let me overcome my weakness and that allow me to pursue my diverse research interests. His valuable assistance, suggestions and support helped me a lot in writing this thesis.

I am also greatly indebted to my second supervisor Prof. Dr. Xiaoming Fu, for all his time, professional advices and guidance. Without his efforts, this thesis would not have been what it is today.

I am deeply grateful to Prof. Dr. Delphine Reinhardt for being a member of my thesis committee; I also thank him, Prof. Dr.-Ing. Marcus Baum, Prof. Dr. Carsten Damm, and Prof. Dr. Stephan Waack for serving as the examination board for me. Their comments made this thesis better.

My thanks in addition go to all the members of Telematics group at the University of Göttingen. The whole group helped me to continuously improve through constructive criticism and reviews, discussions, collaboration, and the enjoyable time in the Group.

Finally, I would like to thank my parents and friends, who always stay by my side and motivate me to move on.

Abstract

As Mobile Ad hoc NETworks (MANETs) grow more popular and are deployed as solutions in various applications such as road safety in Vehicular Ad hoc NETworks (VANETs), wildlife tracking in Wireless Sensor Networks (WSNs) and Device-to-Device (D2D) communications in 5G, the need for efficient routing that is robust against malfunctioning or malicious network nodes is increasing. A fuzzy logic enhanced Ant Colony Optimization (ACO)-based routing algorithm, which addresses these issues, is proposed in this thesis. The Security Aware Fuzzy Enhanced Ant Colony Optimization (SAFEACO) routing protocol makes use of a distributed fuzzy logic module to identify misbehaving nodes and exclude them from the routing process. The SAFEACO routing protocol is implemented in the NS-3 simulator and various experiments have been performed in both MANET and VANET scenarios. The performance of SAFEACO is compared with other modern and widely known approaches. Simulation results show that SAFEACO has superior performance in all relevant metrics, such as packet delivery ratio (PDR) and end-to-end delay. Due to its ability to identify misbehaving nodes, SAFEACO also provides a higher level of robustness against black hole, Sybil and flooding attacks.

Contents

List of Figures

List of Tables

List of Abbreviations

ABPKM	Autonomous Bio-inspired Public Key Management	34
ACECR	Ant Colony based Energy Control Routing	27
ACK	ACKnowledgment	13
ACO	Ant Colony Optimization	3
ACS	Ant Colony System	17
AI	Artificial Intelligence	3
AODV	Ad hoc On-Demand Distance Vector routing	2
BANT	Backward ANT	21
Blocking-ERS	Blocking Expanding Ring Search	24
CA	Certification Authority	30
CBLR	Cluster-Based Location Routing algorithm	15
CBR	Constant Bit Rate	70
DDR	Data Delivery Ratio	43
DSDV	Destination-Sequenced Distance-Vector	2
DSR	Dynamic Source Routing	2
DYMO	DYnamic MANETs On-demand routing protocol	29
DoS	Denial of Service	51
EAACKm	Enhanced Adaptive ACKnowledgment modified version	70
EAACK	Enhanced Adaptive ACKnowledgment	13
EAAR	Energy-Aware Ant based Routing	26
EANT	Error ANT	25
ECC	Elliptic Curve Cryptography	31
EFANT	External Forward ANT	41
FANTStack	Forward ANT Stack	25
FANT	Forward ANT	21
FIS	Fuzzy Inference System	33
FPNT-OLSR	Fuzzy Petri net based Trust model embedded Optimized Link State Routing	13
FTAR	Fuzzy-based Trusted Ant Routing	32
GPSR	Greedy Perimeter Stateless Routing	15

GPS	Global Position System	15
GTS	Guaranteed Time Slot	50
HC-ACO	Hyper-Cube framework for Ant Colony Optimization	17
IFANT	Internal Forward ANT	41
IPv4	Internet Protocol version 4	76
IP	Internet Protocol	53
ITS	Intelligent Transportation Systems	14
MAC layer	Medium Access Control layer	49
MAC	Message Authentication Code	31
MANET	Mobile Ad hoc NETwork	1
MEP	MEmber Packet	29
MMAS	MAX-MIN Ant System	17
MMP	Max-Min-Path	27
MPR	Multi-Point Relay	13
MRA	Misbehavior Report Authentication	13
MRB	Minimum Residual Battery energy	26
NANT	Notification ANT	41
NA	Node Active	33
NHA	Next Hop Availability	24
OLSR	Optimized Link State Routing protocol	11
OSI model	Open Systems Interconnection model	49
PBANT	Proactive Backward ANT	22
PDR	Packet Delivery Ratio	4
PFANT	Proactive Forward ANT	22
POSANT	POSition based ANT colony routing protocol	28
PSO	Particle Swarm Optimization	3
QoRA	QoS Routing protocol for multi-rate ad hoc networks based on Ant colony optimization	25
QoS	Quality of Service	12
RANT	Repair ANT	43
RBANT	Reactive Backward ANT	22
RFANT	Reactive Forward ANT	22
RPBANT	RePair Backward ANT	22
RPFANT	RePair Forward ANT	22
RREP	Route REPly	40
RREQ	Route REQuest	40
RSU	Road Side Unit	1
RWP	Random WayPoint model	27
S-ACK	Secure ACKnowledgment	13

S-AMCQ	Secure Ant based Multi-Constrained QoS routing algorithm	30
SAFEACO	Security Aware Fuzzy Enhanced Ant Colony Optimization routing protocol	4
SA	Simulated Annealing	27
SBDT	Swarm Based intrusion detection and Detection Technique	33
SDS	Stochastic Diffusion Search	3
SI	Swarm Intelligence	3
SNMP	Simple Network Management Protocol	25
SNR	Signal-to-Noise Ratio	58
SOM	Smallest Of Minimum	33
SPA-ARA	Secure Power-Aware Ant Routing Algorithm	31
SPAN	Smart Phone Ad hoc Network	1
SRP	Source Routing Protocol	32
SUMO	Simulation of Urban Mobility	69
UANT	Update ANT	43
UDP	User Datagram Protocol	76
UMB	Urban Multi-Hop Broadcast protocol	15
V2I	Vehicle-to-Infrastructure	30
V2V	Vehicle-to-Vehicle	47
VANET	Vehicular Ad hoc NETwork	1
VNMG	Vehicular Network Movement Generator	29
VoEG	VANET-oriented Evolving Graph	30
WSN	Wireless Sensor Network	1
ZOR	Zone Of Relevance	15
ZRP	Zone Routing Protocol	11

Chapter 1

Introduction

With the advancing development of technology, laptops, smartphones, tablets and other intelligent mobile devices are commonly seen in daily life. In the survey [1], the results show that smartphones are increasingly common around the world. For example, the percentage of adults in United States who own a smartphone has increased from 56 % to 77 % in the period from 2013 to 2018 and 94 % of adults in South Korea have at least one smartphone which makes South Korea be ranked first place. Sweden has the highest smartphone ownership rate, 80 %, among the European countries. With a 72 % ownership rate, Germany, United Kingdom and Chile are placed joint tenth. In addition, China is at the 15th place which has a 68 % of smartphone penetration. The average smartphone ownership rate across the 39 countries surveyed is 59 %. Smart devices are intelligent and can provide many different types of services to people which make the life more comfortable, convenient and enjoyable. Traditionally, these mobile devices can connect to infrastructure-based networks, such as cellular networks, wired networks and WiFi hot spots. At the same time, these devices can also form what is called Mobile Ad hoc NETwork (MANET) [2], which does not require infrastructure. Generally speaking, MANETs consist of wireless mobile devices which can join and leave the network freely. Due to the lack of infrastructure, a MANET can be deployed with obviously lower costs in comparison to those required by deploying a wired network. For example, mobile devices can connect with each other directly via Bluetooth or WiFi and there is no additional requirements for cables, routers or other types of infrastructure-based equipments. There are many different types of MANETs. For example, the Wireless Sensor Network (WSN) [3] is a type of MANETs which has been applied in many fields. WSNs can monitor environmental measurements, such as temperature, humidity, air pollution and so on. Another example is the Vehicular Ad hoc NETwork (VANET) [4]. In a VANET, vehicles communicate directly with each other or with a Road Side Unit (RSU) to exchange road information to support road safety. In recent years, flying ad hoc networks have been developed. This type of MANETs consists of a number of unmanned aerial vehicle and can be applied for disaster rescue operations. In order to provide an alternate means for information dispersal when all other infrastructure is unavailable, the Smart Phone Ad hoc

Network (SPAN) project is initiated by the MITRE [5]. This project utilizes MANET technology to provide communication between individuals when the communication via all other infrastructure is unavailable. A group of smartphones can leverage primarily Bluetooth and WiFi technology to create SPANs without relying on network infrastructure such as cellular carrier networks and wireless access points. Different from the cellular spectrum, Bluetooth and WiFi technology which is used to connect smartphones requires no special license according to the regulations of most jurisdictions. Furthermore, smartphones can freely join and leave these networks, thus the set up and tear down of SPANs are dynamic and flexible. Due to the high smartphone ownership rate, a SPAN can be conveniently applied in many daily life scenarios. SPANs are good solutions of supporting communication in developing nations where network infrastructure does not exist. For example, the deployment of infrastructure-based networks in a mountain area normally is difficult and cost intensive, but SPANs can enable communications with a lower cost in this area. SPANs are also very useful in natural disasters or terrorist incidents. For example, after a earthquake the existing infrastructure-based networks, for example, cellular networks, may be destroyed and overloaded. SPANs can keep mobile devices connected and aid people during disaster relief operations. Moreover, in temporary large-scale events, for example, music festivals in which huge scale is needed but only for a short period of time, the price-performance ratio of applying SPANs in this case is better than that of using the infrastructure-based networks. SPANs can also be used by protesters as a communication tool, using mobile applications, such as FireChat [6], which allow users to exchange messages and pictures via MANETs.

1.1 Research Question

MANET applications bring many benefits and make life more comfortable and convenient. However, to gain all these benefits efficient and secure communication between nodes in MANETs is required. Therefore, routing protocols which fulfill the requirements of MANET applications are desired. Since the 1990s, many state-of-the-art routing protocols have been proposed for MANETs, such as Destination-Sequenced Distance-Vector (DSDV) [7], Ad hoc On-Demand Distance Vector routing (AODV) [8] and Dynamic Source Routing (DSR) [9]. However, these routing protocols proposed long time ago focus on solving basic routing requirements and can hardly fulfill the various new requirements of MANET routing nowadays. Besides the basic routing requirements, new routing protocols designed for MANETs are supposed to work in a self-organizing manner and provide low packet delay, high packet delivery rate and effective adaptation to network topology changes with low control overhead.

Since biologists and nature scientists have found that activities in many biological systems such as ant colonies and bee colonies are based on simple rules and don't rely on any centralized control structure [10], many meta-heuristics inspired by biological systems have been introduced by different scientists in the past two decades. G. Beni and J. Wang introduced the expression of

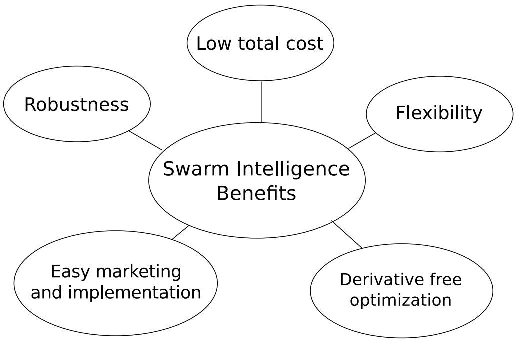

Low total cost
Robustness
Flexibility
Swarm Intelligence Benefits
Easy marketing and implementation
Derivative free optimization

Figure 1.1: Swarm intelligence benefits.

Swarm Intelligence (SI) in their research of cellular robotic systems in 1993 [11]. The concept of SI is employed in work on Artificial Intelligence (AI). SI is a computational intelligence technique which is based on the collective behavior of decentralized, self-organized systems [12]. A typical SI system is made up of a group of simple agents which interact locally with each other and with the environment surrounding them [13]. Agents in an SI system follow simple rules and act without the control of any centralized entities. However, the social interactions between such agents often lead to smart global behavior. A. K. Kordon pointed out in [12] the main advantages of applying SI which are shown in figure 1.1. By fully taking advantage of the swarm, SI systems are able to provide optimized solutions, which ensure high robustness, flexibility and low cost, for large-scale sophisticated problems without a centralized control entity [12]. Stochastic Diffusion Search (SDS) [14], Particle Swarm Optimization (PSO) [15] and Ant Colony Optimization (ACO) [16] are some well-known meta-heuristics in field of SI.

The ACO algorithm is inspired by biology and follows the approach that ants use in finding efficient paths, by tracking pheromones deposited along the way. It applies just as well in networks as it does in nature and presents a common framework for approximating solutions to NP-hard optimization problems [17]. Due to the dynamic nature of ACO's connectivity, ACO is able to continuously adapt to network changes in real time [18]. Moreover, the artificial ants can find multiple solutions simultaneously for the considered problem [17]. Therefore, ACO based algorithms are able to efficiently find optimal routes, which has lead to them been applied in the field of routing for network communication.

As the value of MANET applications increases the motivation of attackers to manipulate or disrupt them also increases. In critical MANET applications, it is always likely to have adversaries, who aim to disrupt the network or discover private information on the network. For example, malicious vehicles in VANET scenarios can broadcast fake road safety messages which could possibly cause traffic jams or even accidents. In such environments, human life can be endangered if the network is not operating correctly due to attacks. Moreover, some of the nodes in a MANET might act selfish in the routing process to save their battery power or data storage. Therefore, the design of routing protocols plays an important role in protecting security in MANETs. The goal of this thesis is to design an efficient routing protocol in MANETs that can provide not only high Packet Delivery Ratio (PDR), low end-to-end delay and low overhead, but also can be robust against malfunctioning devices and malicious network participants.

1.2 Thesis Contributions

The main contributions of this thesis can be summarized as follows:

- Review of the existing ACO based routing protocols in MANETs from 1998 up to now, the classification of reviewed ACO based routing protocols, the comparative analysis in terms of protocol design and simulation related parameters for all reviewed protocols, the summary of the development of ACO based routing protocols and the discussion of the open issues and the possible future research directions in this field.
- Modeling and implementation of Security Aware Fuzzy Enhanced Ant Colony Optimization routing protocol (SAFEACO) which aims to find optimal routes while also detecting and isolating suspicious nodes in MANETs.
- Further development and implementation of SAFEACO in VANET scenarios.
- Implementation of three selected types of network layer attacks for the evaluation.
- Experimental analysis and evaluation of the proposed SAFEACO routing protocol in both MANET and VANET scenarios with respect to several performance metrics.

1.3 Impact

During the course of this work, a survey paper which reviews the existing ACO-based routing protocols in MANETs has been published in the following peer reviewed journal:

- H. Zhang, X. Wang, P. Memarmoshrefi, and D. Hogrefe, "A survey of ant colony optimization based routing protocols for mobile ad hoc networks," IEEE Access, vol. 5, pp. 24 139–24 161, 2017. [Online]. Available: `http://doi.org/10.1109/ACCESS.2017.2762472`

In addition, the main articles which include the primary idea and the intermediate results have been published in the following peer reviewed conference proceedings:

- H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "A Security Aware Fuzzy Enhanced Ant Colony Optimization Routing in Mobile Ad hoc Networks," in Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2018.

- H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "A security aware fuzzy enhanced reliable ant colony optimization routing in vehicular ad hoc networks," in 2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018, pp. 1071–1078. [Online]. Available: `http://doi.org/10.1109/IVS.2018.8500485`

- H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "Employing Fuzzy Logic to Provide Security Awareness in ACO Routing for MANETs," in Wireless Communications and Networking Conference (WCNC). IEEE, 2018.

1.4 Thesis Scope

Chapter 1 gives an introduction to the studied problem and emphasizes the main contributions of the thesis. The thesis scope gives an overview of the content in the thesis.

Chapter 2 introduces the theoretical foundations of this thesis as shown in figure 1.2. Section 2.1 presents an overview of the existing routing protocols in both MANETs and VANETs. Section 2.2.2 first presents the basis of the Ant Colony Optimization (ACO) algorithm and ACO-based routing algorithm in MANETs. Then, a review of the existing ACO-based routing protocols in MANETs is presented based on five main categories in section 2.2.3. A comparative analysis of the reviewed protocols in each category is presented in the form of different tables which display design related parameters in section 2.2.4. Another comparative analysis that focuses on simulation parameters and a general discussion of the open issues and possible future research directions in the field of ACO-based routing protocols are given in section 2.2.5. After the review of the ACO-based routing protocols in MANETs, a brief introduction of attacks in MANETs is presented in section 2.3. Finally, the three network layer attack models which are applied for evaluating the performance of SAFEACO in chapter 5 are introduced in section 2.4.

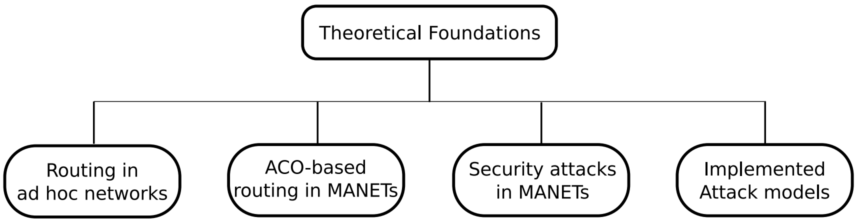

Theoretical Foundations
Routing in ad hoc networks
ACO-based routing in MANETs
Security attacks in MANETs
Implemented Attack models

Figure 1.2: Theoretical foundations.

Chapter 3 first introduces the routing mechanism of SAFEACO in detail. Reactive route setup, proactive route maintenance, data transmission and the handling of link failures in SAFEACO are explained in detail in section 3.1, 3.2, 3.3, and 3.4. Then the fuzzy based malicious behavior detection system which includes the input and output values, the fuzzy rules and the fuzzy inference system are presented separately for MANET and VANET scenarios in section 3.5.2 and

3.5.3.

Chapter 4 introduces the network simulator and tools which are used for the experiments. All the implementation related parameters are given in detail based on the network types in section 4.2 and 4.3.

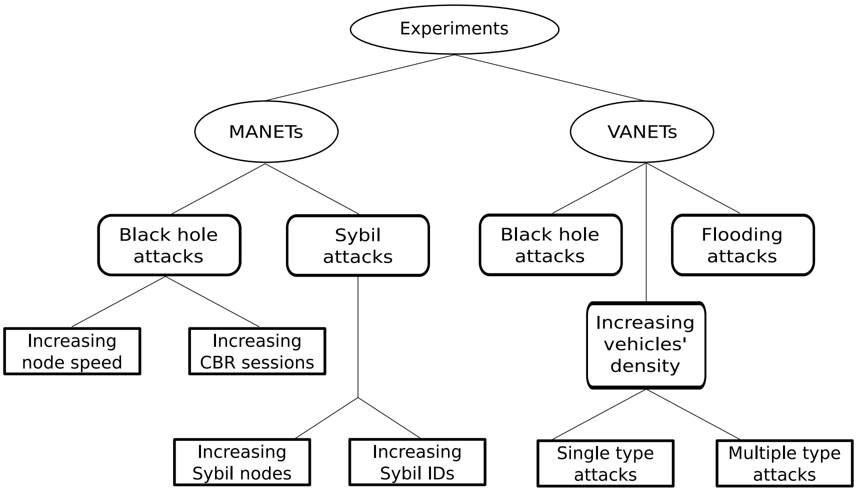


Figure 1.3: Simulation experiments design.

Chapter 5 presents the experimental analysis and evaluation of the proposed SAFEACO scheme regarding several performance metrics. The simulation experiments are designed separately for two scopes: MANET and VANET scenarios. For MANET scenarios, the performance of SAFEACO is investigated under black hole and Sybil attacks. For the latter, black hole and flooding attacks are both applied during the investigation. Figure 1.3 gives an overview of the simulation experiments in this thesis. More details of the experimental series can be found in table 5.1 and 5.7 in chapter 5. Section 5.2 presents the performance results based on the black hole and Sybil attacks in different MANET scenarios. Section 5.3 shows the performance results based on the black hole and flooding attacks in different VANET scenarios. The discussion sections 5.2.3 and 5.3.5 in this chapter also summarize the overall performance of SAFEACO in both MANET and VANET experiments.

Finally, Chapter 6 concludes the work and presents a brief discussion of the possible future directions for the research.

Chapter 2

Theoretical Foundations

The main objective of this chapter is to introduce the theoretical foundations of this thesis. First, the routing algorithms in wireless ad hoc network are introduced. Then, the ACO algorithm and a review of the existing ACO-based routing protocols for MANETs are presented. The fuzzy logic algorithm and the network security challenges are explained afterwards. At the end, the three network layer attack models, which are applied in the experiments, are presented.

2.1 Routing in Wireless Ad Hoc Networks

With the emergence of portable smart devices and the development of technology in wireless communications, wireless applications have expanded very fast in the past few decades. The flexibility of wireless ad hoc networks, and the absence of network infrastructure makes this kind of networks easier and cheaper to put into place than traditional wired networks, which need a suitable system of cables. These properties enable creating considerable commercial applications. Wireless applications enable users to have rapid access to information independent of time or place, and therefore such kind of wireless applications is getting more and more popular. The demands of self-organization, independence, adaptability, and cost reduction in wireless applications have encouraged researchers to find solutions for improving many functions of wireless networks. MANET which effectively meed these demands are a proper solution.

2.1.1 MANETs

MANET [2] is an autonomous system of mobile nodes and associated hosts connected by wireless links, without the need for the infrastructure support or a centralized administration. Nodes in such network act also as routers. Furthermore, these nodes are free to move and organize themselves arbitrarily. Therefore, the prediction of the high dynamic network topology changes is very difficult.

In comparison with the wired networks, MANETs are more flexible and robust and they are able to deal with node mobility. Since MANETs do not require any infrastructure support or a central administration, the deployment of MANETs is very simple and a new MANET becomes operational the moment all wireless terminals are presented in the given space. In certain environments where wired networks are not available, such as natural disasters, MANETs are the only available means of communication and access to information. Moreover, MANETs also play an important role in applications for civil recreations, conferences, and so on. MANETs also can be considered as a wireless Internet network. Therefore, users of MANETs can move geographically while keeping the connection with the rest of the world.

The principal characteristics of MANETs are summarized as below [2]:

Lack of infrastructure:

A key difference between MANETs and the other types of mobile networks is that there is no preexisting infrastructure or any form of centralized administration in MANETs. The establishment and maintenance of the network connectivity are handled by the mobile nodes in a self-organized manner.

Dynamic topology:

As introduced before, nodes in MANETs can move randomly and they can also freely join or leave the network at any time. As consequence, the changes of the network topology are rapid and unpredictable.

Limited bandwidth and variable capacity of links:

Since the wireless transmission channel is shared, bandwidth in MANETs is restricted in comparison with the one offered by the wired networks. Congestion is a major problem caused by the limited bandwidth.

Energy constraints:

Mobile nodes are usually equipped by autonomous energy sources, such as batteries. Since the energy in batteries is limited, the energy consumption is important as it affects the life expectancy of the network.

Limited security:

In the classic wired networks, the central administration can take care of the security issues for the whole network. However, due to the absence of infrastructure, there is no such administrative node in MANETs. Therefore, it's more difficult to ensure the security in MANETs than in classic wired networks.

2.1.2 Routing in MANETs

Generally speaking, routing is the process of selecting a path for transmitting information to the targeted destination in a network. In wired networks, routers are responsible for determining the path for packet transmission. However, there is no such type of nodes in MANETs. Wireless communication in MANETs is carried out directly between neighboring nodes or via intermediary nodes. Packets are delivered hop by hop. Every node in MANETs acts as a router, and retransmits packets to the next hop when it becomes the intermediate node in the paths of the other nodes. Routing in MANETs is therefore the process of searching the best path from source to destination. The main challenge for routing protocols in MANETs is to deal with the nodes' mobility while considering the limited network resources, such as bandwidth and energy [19]. Due to the absence of infrastructure, every node must take part in the route discovery and maintenance processes to the other nodes. Another essential issue for the routing protocols is to reduce the routing overhead despite the increasing number of nodes and their mobility [19]. There are many different ways to classify the routing protocols in MANETs. By considering the method used to discover and maintain routes, these protocols can be classified as proactive, reactive and hybrid [19].

Proactive routing

Every node in the proactive routing protocols such as the DSDV protocol [20] and Optimized Link State Routing protocol (OLSR) [21], regularly maintains the up-to-date routing information in its routing tables, no matter whether it has any data packets to send. The end-to-end packet delay in this type of routing protocols is usually low, since the data packets at the source nodes can be sent out at once without waiting for the route discovery process. However, in order to maintain the up-to-date global view of the network, any change in the network topology triggers updates in the routing tables. Therefore, the signalization which affects the bandwidth is a challenge in such routing protocols. Furthermore, in large networks or in networks which have frequent and rapid topological development, the routing overhead in this type of routing protocols is relatively high.

Reactive routing

Different from the proactive routing protocols, a node in the reactive routing protocols such as AODV [8] and DSR [9] starts the route discovery process only when it has data packets to send and there is no valid route in the routing table. The advantage of these protocols is that the routing overhead caused by the regular updates in the routing tables is reduced. However, the end-to-end packet delay in this type of routing protocols is relative high, as there is no routing information when the data packets arrive at the source nodes.

Hybrid routing

Hybrid routing protocols attempt to combine the advantages of the proactive and reactive protocols. An example in this category is Zone Routing Protocol (ZRP) [22]. In ZRP, the routing mechanism applied by the nodes depends on whether the destination node is located inside the predefined zone. Before the data transmission, source nodes decide the size of the zone in which the proactive routing mechanism is applied, for example within three hops. In this case, source node maintains all existing routes information in its routing table for all nodes within its three hop zone and the reactive routing mechanism is triggered when the destination node is outside this zone.

Over the past two decades, researchers have proposed various routing approaches. In the early development phase of MANETs, these protocols were considered to be state of the art protocols and were sufficient to satisfy the demands of MANET applications. However, there are also some shortcomings in the existing routing protocols in MANETs as pointed out in [19]: First, these routing protocols have not covered all routing problems, for example reducing delay, data drop ratio, and the network load. Secondly, many of them use only the best route for data delivery and there is no alternative route when the primary route has congestions. Furthermore, they do not concern with link reliability, such as the available bandwidth, end-to-end delay and energy consumption. Finally, most of them do not consider the efficiency of the route, as they aim to find any route, not the optimal route, from the source node to the destination node.

In order to satisfy the increasingly higher levels of requirements by the advanced MANETs applications, routing protocols in MANETs are suggested to provide high efficiency in adapting to the frequent topology changes in MANETs and to consider the Quality of Service (QoS) merits such as end-to-end delay and energy consumption in the route discovery process [19]. Instead of searching the shortest route, they should find the optimal routes which consider multiple routing merits, such as bandwidth and packet losses. Furthermore, they should also be able to provide an alternative route in case the primary one fails. The overhead made by the control packets is suggested to be kept as low as possible. Finally, the security threatens in the routing process should also be considered. Researchers are encouraged to design new routing protocols, which could provide higher packet delivery ratio, lower end-to-end delay and less overhead, while also providing high levels of security.

The ACO meta-heuristic is inspired by the foraging behavior of ants in nature. It presents a common framework for approximating solutions to NP-hard optimization problems [17]. Due to the dynamic nature of ACO's connectivity, ACO is able to continuously adapt to network changes in real time [18]. Moreover, the artificial ants can find multiple solutions simultaneously for the considered problem [17]. Therefore, ACO-based algorithms are able to efficiently find optimal routes, which has lead to applying them in the field of routing for network communication. A review of the existing ACO-based routing protocols in MANETs is given in section 2.2.3. Although ACO-based routing mechanism can efficiently find the optimal routes in dynamic networks, it can not inherently defend against the network layer attacks. Researchers have also proposed several protocols which consider the security related parameters in the route discovery process. These security aware ACO-based routing protocols are introduced in section 2.2.3.

Besides these security aware ACO-based routing protocols, there are also other approaches which are based on state-of-the-art routing protocols. Enhanced Adaptive ACKnowledgment (EAACK) which was proposed by Shakshuki et al. [23] in 2013 is one of the widely cited approaches in the recent years. It is based on the DSR [9] protocol and employs an enhanced adaptive acknowledgment scheme to detect malicious nodes. EAACK shows better performance than DSR, AACK [24] and TWOACK [25] with respect to both overhead and PDR. However, the authors do not evaluate the end to end delay of EAACK. Since EAACK is based on DSR, its reactive routing mechanism should lead to a higher amount of delay than it would be present in a hybrid scheme. EAACK's misbehavior detection system consists of three phases applied in sequence: ACKnowledgment (ACK), Secure ACKnowledgment (S-ACK) and Misbehavior Report Authentication (MRA). ACK is an end-to-end acknowledgment scheme. If ACK fails, S-ACK and MRA are trigged. S-ACK is used to detect misbehaving nodes and generate misbehavior reports. MRA mode is applied to authenticate the misbehavior reports. This hierarchical detection system leads to additional delay. Moreover, the application of MRA requires that the source node has at least one alternative route to the destination node. However, in a highly dynamic network, this is not guaranteed. If there exists no alternative route, the source node has to find a new route, which leads to further delay.

Tan et. al proposed the Fuzzy Petri net based Trust model embedded Optimized Link State Routing (FPNT-OLSR) protocol which is a trust based routing mechanism for secure routing in MANETs in 2015 [26]. In FPNT-OLSR four trust factors are defined for evaluating the nodes behavior in both route discovery and data delivery process. A Multi-Point Relay (MPR) node monitors its neighborhood and evaluates the trust value of a target node by using the proposed trust reasoning model based on the collected trust factors. Later the trust value is propagated as recommendation in the network. After receiving multiple recommendations, the node should aggregate all these recommended trust values and its own direct trust values into the overall trust values. Since FPNT-OLSR is a proactive routing protocol, a node updates its trust based routing table regularly. The routes in the routing table are sorted by the overall trust values of the routes. Although FPNT-OLSR can provide secure routes in MANETs, there are still some shortcomings. First, without the recommended trust values from the MPR nodes, a normal node can not update its trust based routing table. In case that a node has selected only one MPR node which is malicious, this node is hard to find any secure route to any other nodes in the network. In case that a node has selected more than one MPR node, the node has to wait for all the recommendations from the chosen MPR nodes and aggregate them to the overall trust values. This causes a delay of updating the routing table. Furthermore, the recommendation based system is vulnerable to the Sybil attack which can create multiple identities and flood the a huge amount of fake recommendations. Secondly, the energy consumption and the congestion at the MPR nodes need to be considered, since MPR nodes are responsible not only for searching routes and sending the topology control packets, but also for evaluating and propagating trust values. If there is no counter measurement, the MPR nodes should run out of power much earlier than the normal nodes. Selecting new MPR nodes leads to more overhead and end-to-end delay. Thirdly, as in all other proactive routing protocols, the regularly updates of the trust values and the routing tables lead to the communication overhead. Finally, despite the trust reasoning model and the trust propagation process which are applied to detect the malicious nodes, FPNT-OLSR does not change the basic routing structure of OLSR. The experiments results with apparent fluctuations in scenarios without malicious nodes are not very convincing. Although OLSR is an efficient routing protocol in MANETs [26], the results of the different series of experiments made by Ducatelle show that AntHocNet is more efficient than OLSR. Therefore, the AntHocNet routing structure is applied in the proposed SAFEACO. More details are presented in chapter 3.

Since VANETs are a special type of MANETs, some of the MANET routing approaches can be applicable to VANET scenarios, such as the proposed SAFEACO in this thesis. The next section will give a short overview of the routing in VANETs.

2.1.3 Routing in VANETs

Besides routing protocols which are designed for MANETs, researchers have also proposed many routing protocols for VANETs due to the increasing number of new applications in VANETs. VANETs [4] consist of collections of mobile vehicles and are becoming a new emerging branch of wireless technology which are derived from MANETs [27]. Although VANETs have several similarities to MANETs, they are distinguished from other kinds of MANETs by their vehicle movement properties (e.g. high speed), hybrid network architectures and practical application scenarios. There are various applications for VANETs, the main one being Intelligent Transportation Systems (ITS) [28]. ITS is not a single application, but rather includes a variety of applications, such as co-operative traffic monitoring, the control of traffic flows, prevention of collisions, nearby information services, providing Internet connectivity to vehicles and so on [28]. Due to the high mobility and unreliable channel conditions, VANETs have many unique characteristics, which pose many challenging research issues when implementing its functionalities, such as data dissemination and data sharing [28]. Security is another important issue, as unreliability might lead to dangerous situations in road traffic. As the applications in VANETs become increasingly more widespread, attackers are also more motivated to manipulate or disrupt the communications in VANET applications. Therefore, the design of efficient and secure routing protocols for VANETs is very important. However, due to the dynamic nature of the VANETs, discovery and maintenance of routes is a very challenging task. To solve this issue, a variety of different routing protocols have been proposed. They generally fit into five categories: ad hoc, position-based, cluster-based, broadcast, and geocast routing [28].

Ad hoc routing

Ad hoc routing protocols for VANETs are mainly the ones which are originally designed for MANETs, such as the AODV [8] and DSR [9]. VANETs have many similarities to other types of MANETS, such as not relying on fixed infrastructure, having low bandwidth, short radio transmission range and so on. However, vehicles in VANETs move much faster than the normal mobile nodes in MANETs, which can lead to poor performance of MANET routing algorithms in VANETs.

Position-based routing

In position-based routing protocols, nodes use location information to help facilitate communications. For examples, in greedy routing nodes always forward the packets to the node that has the shortest geographical distance to the destination. Greedy Perimeter Stateless Routing (GPSR) [29] is one of the representative position-based protocols in literature. In GPSR there is no need to establish a global route from source nodes directly to destination nodes, which can reduce the processing costs of system. In city scenarios however, GPSR can suffer from several problems, due to the presence of obstacles and mobility leading to routing loops [28].

Cluster-based routing

Cluster-based routing attempts to provide scalability by creating a virtual hierarchical network infrastructure through the clustering of nodes. Vehicles are divided into clusters with cluster heads that coordinate intra- and inter-cluster communications. While vehicles inside a cluster communicate with each other directly, the communications between clusters are performed via the cluster-heads or the cluster gateways. Santos et al. [30] have proposed a Cluster-Based Location Routing algorithm (CBLR) for VANETs. It assumes that all nodes can gather their position information by Global Position System (GPS) to build the clusters. Simulation results show that CBLR can achieve good scalability for large networks. However, forming and maintaining clusters causes extra overhead. Moreover, cluster-based routing protocols also rely on the geographical information of vehicles to create stable clusters, which may not always be reliable or available.

Broadcast routing

Broadcast routing protocols, such as Urban Multi-Hop Broadcast protocol (UMB) [31], transmit data to all available nodes within communication range over the entire network. This kind of routing performs relatively well for VANETs with a limited small number of vehicles and is easy to implement. However, when the number of vehicles in the network increases, the bandwidth requirements increase exponentially [28]. Moreover, since each node receives and re-broadcasts every message almost at the same time, it leads to packet collisions and network congestion, which may cause a high amount of additional overhead.

Geocast routing

Geocast routing [32] is basically a location-based multicast routing approach that aims to deliver packets from a source vehicle to all other vehicles within a predefined geographical zone. While useful for use cases such as emergency broadcasts, the communication range is limited by Zone Of Relevance (ZOR) and it is mainly designed for unidirectional message dissemination in one single region, not for pairwise communication in the network.

2.2 Ant Colony Optimization (ACO) algorithm

Inspired by the foraging behavior of ants in nature Dorigo et. al proposed the ACO meta-heuristic which presents a common framework for approximating solutions to NP-hard optimization problems [17]. The details of ACO routing algorithm [33] is introduced in section 2.2.2. A review of the existing ACO-based routing protocols in MANETs [33] is presented afterwards.

2.2.1 Basis of ACO algorithm

Before introducing the ACO routing algorithm in MANETs, the background information of the nature ants and the artificial ones is presented first.

Ants in nature

Ants are ubiquitous insects which began to diversify 100 million years ago [34]. Now, more than 8800 known species of ants [35] still exist across the globe. In nature, ants are well-known type of social insects. The size of an ant colony can vary from a few dozen to millions. In an ant colony, there are usually different castes. "Workers" are the most common ants which could be found in any colony. They are small sterile females that take over most of the work in the colony: foraging food, maintaining and expanding the nest, taking care of the queen and brood, and so on. "Queens" are the fertile females which are the founders of all colonies. The main task of a queen is to lay eggs. "Drones" are the only male ants in a colony and they only survive during the mating season. In some special ant colonies, there could also be other castes, such as "soldiers", which are larger and stronger than typical "workers". As the name indicates, "soldiers" protect their colony from predators. Although each caste in the colony has different tasks, all castes work together collectively to ensure the colony's survival [36], [37]. It's well-known that a single ant is not very bright, but ants in a colony can finish remarkable tasks, such as dealing with floods. In [38] researchers have found that ants can link their body to build self-assemblages. For instance, in order to beat floods, fire ants are able to use their bodies to build rafts in short time. N. J. Mlot et al. have also measured the strength and speed by which ant rafts are built in another study [39]. It shows that thousands of ants can rearrange themselves to build a stable raft within 200 seconds, and ants can use a force of 400 times their own weight to keep the raft. Observations in [39] and [40] show that ants can react to their environment quickly and survive under adverse environmental conditions.

Different from human, ants rarely use sound or sight to exchange information with each other. Instead, ants produce volatile chemical substance which is known as pheromone. Pheromone is the key component of ant's communication. While moving around, ants lay pheromone through their glands along their path and ants use their antennas to detect the pheromone in the surrounding area.

There are different types of pheromone perfumes which represent different chemical words that the whole ant colony understands. Ants react differently corresponding to the type of pheromone detected. For instance, in order to alarm nest-mates, some species of ants create alarm pheromones by using their poison glands [41]. This kind of alarm pheromone includes two components: formic acid and n-undecane. By detecting the alarm pheromone, worker ants either escape fast or go towards the danger, in case that they are the defenders of the colony. Another well-known type of pheromone is the trail pheromone. This kind of pheromone is used by ants while foraging. An ant foraging for food leaves its nest and chooses randomly a direction to move on, as far as it doesn't find a pheromone trail. If it finds one, it has a high probability to follow the trail. No matter which decision it has made, it deposits pheromone over its route. Once it find the food, it returns to the nest and reinforces its trail. Other ants which detect its trail will follow the trail with great probability and lay more pheromone over it. This is a positive feedback loop system since the higher the trail's pheromone, the higher the probability of an ant to follow the trail. When the food is exhausted, no more pheromone is deposit on the trail and the pheromone begins to evaporate over the time. This negative feedback behavior supports ants to adapt to the dynamic environment [18].

From nature to artificial ants

Assemblages of ants take on similar functions like those existing in the human societies, but ants don't rely on any central control to provide these functions. Therefore, understanding how the systems of ant colonies work has long been an attractive subject of study. In the 1980s, F. Moyson and B. Manderick studied self-organization behavior among ants [42]. S. Goss et al. proposed the initial idea of ant colony optimization algorithms based on their study of the collective behavior of ants in [43]. In this work, the author designed a simple, yet brilliant experiment: the double bridge experiment. In this experiment, an ant nest and a food source are connected by a double bridge which consists of two bridges with different lengths. The experiment's results indicate that the short path attracts more ants to follow, if both short and long paths are given to the ants in the same time. Moreover, the short path attracts much less ants, if it is given after the long path is followed by the ants for a while. This indicates that the pheromone evaporation rate controls the trade-off between path-exploration and path-exploitation [18]. Based on the foraging behavior of ants, M. Dorigo initially proposed the ACO algorithm, the first ant-inspired algorithm aimed to find an optimal path in a graph, in his dissertation and published it in 1992 [16]. In cooperation with L. M. Gambardella, M. Dorigo proposed Ant Colony System (ACS) in 1997 [44]. Since then, research in this area was followed by many other scientists and many popular variations of ACO algorithms were proposed. B. Bullnheimer, et al. proposed the Rank-based Ant System in 1997 [45]. V. Maniezzo introduced ANTS: exact and approximate nondeterministic tree-search procedures for the quadratic assignment problem in 1999 [46]. T. Stützle and H. H. Hoos invented MAX-MIN Ant System (MMAS) [47] in 2000. C. Blum et al. proposed Hyper-Cube framework for Ant Colony

Optimization (HC-ACO) in 2004 [48].

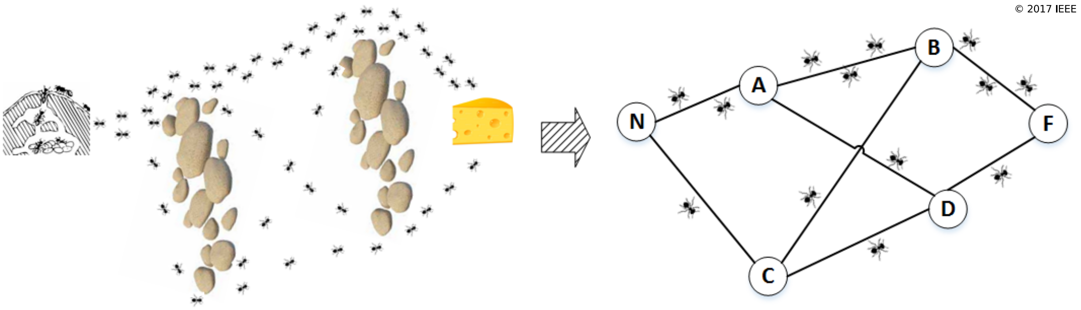
The ACO meta-heuristic which belongs to the field of SI is inspired by the foraging behavior of ants in nature. In ACO meta-heuristic, artificial ants work together to find good solutions for difficult combinatorial optimization problems [17]. Recall in the nature case, an ant deposits pheromone on its traveled path to mark its trail and inform other ants. When subsequent ants find a trail, they have a high probability to follow it. Once a subsequent ant follows the trail, it lays down new pheromone over the path. As consequence, the pheromone of the trail is reinforced and it might attract more ants to follow. Therefore, the pheromone represents the indirect information exchange between the individual ants.

In order to apply ACO algorithm to solve an optimization problem in real life, the considered problem firstly needs to be represented in a way that each potential solution of the problem is a path in a construction graph [49]. For example, the problem of how to find the optimal path between the ants' nest and the food source can be represented in a construction graph as shown in figure 2.1. Thus, the initial problem is mapped to the new problem on how to find the optimal path between node N and node F.

2.2.2 ACO-based routing protocols in MANETs

After finding the construction graph, the constraints of the problem should be defined. In this case, the constraint is that ants can only move on the arcs which connect the nodes in figure 2.1. Each arc in figure 2.1 can have associated pheromone trails and a heuristic value [17]. The pheromone trail represents a long-term memory about the ant search process. For each destination there is a separate pheromone trail assigned to the arc. In contrast, there is only one heuristic value at each arc and it is a prior knowledge about the problem instance or run-time information provided by other sources. In many cases, this value is the cost of adding the arc to solution under construction.

In this example, the solution construction is straightforward: every ant in this construction graph starts at a single node N and aims for the same destination node F. Ants follow a probability



© 2017 IEEE

Figure 2.1: A representation example of ACO meta-heuristic.

decision rule to exploit the network. This probability rule is a function of local pheromone trails and heuristic information, and it can also be related to the ant's private memory and the problem constraints [17]. The common applied probability rule [50] can be represented as equations (2.1) and (2.2):

$$P_{ij}(t) = \begin{cases} \dfrac{[\tau_{ij}(t)]^{\alpha} \cdot [\eta_{ij}]^{\beta}}{\sum_{l \in N_i} \left[\tau_{il(t)}\right]^{\alpha} \cdot [\eta_{il}]^{\beta}}, \text{ if } j \in N_i & (2.1) \\ 0 \qquad\qquad\qquad\qquad , \text{ if } j \notin N_i & (2.2) \end{cases}$$

$P_{ij}(t)$ is the probability of an ant to move from node i to node j at the t^{th} iteration step or time slot; N_i is the set of current neighboring nodes of node i; $\tau_{ij}(t)$ is the pheromone intensity on the arc between node i and j at t^{th} iteration step or time slot; η_{ij} is the heuristic information of the arc between node i and j and it's usually a non-increasing function of moving cost from node i to node j; α and β are weight parameters which control the relative impact of pheromone intensity $\tau_{ij}(t)$ versus heuristic information η_{ij}. If α value is high, then the pheromone intensity has strong impact to ants. In this case ants are more biased to follow the path which is chosen popularly by previous ants. This further leads to a situation in which all ants would eventually construct the same path. If α value is low, then the ACO algorithm is close to a stochastic greedy algorithm. When $\alpha = 0$, ants select the next hop node only based on the heuristic information, eg. cost. In contrast, ants are attracted only by the pheromone intensity when $\beta = 0$. Equation (2.2) shows that ants can only move to the neighboring nodes.

Once an ant leaves node N, it moves to one of its neighbor nodes according to equation (2.1). Every artificial ant has a memory space which is used for storing path related information, such as the nodes visited in its trip. An artificial ant moves hop by hop until it reach the destination node F or another terminal condition is satisfied, for example the maximum travel hop count of the ant is reached. If the ant finds the destination node F, it retraces exactly the same path backward to the start point, node N. Once an ant has constructed a solution, or while building a solution, the ant evaluates the solution or partial solution to decide the amount of pheromone updates.

The update of pheromone trail can be either increased or decreased. The pheromone update amount assigned to an arc is calculated based on the quality of a solution in which this arc is involved, and the pheromone evaporation rate, as shown in equation 2.3 [50].

$$\tau_{ij} \leftarrow (1-\rho) \cdot \tau_{ij} + \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \tag{2.3}$$

τ_{ij} is the pheromone value laid by ants on the arc of node i and node j, namely $arc(i,j)$; $\rho \in (0,1]$ is the pheromone evaporation rate; m is the number of ants; $\Delta\tau_{ij}^{k}$ is the amount of pheromone reinforcement deposited by the k^{th} ant for the $arc(i,j)$ [50]:

$$\Delta\tau_{ij}^{k} = \begin{cases} Q/C^{k}\text{ , if } arc(i,j) \in P^{k} & (2.4) \\ 0 \quad\quad\text{ , if } arc(i,j) \notin P^{k} & (2.5) \end{cases}$$

Q is a positive application-specific constant; P^k is the set of arcs chosen by the k^{th} ant in its path; C^k is the overall cost function of the current path which is constructed by the k^{th} ant. For example, C^k can be the length of the path constructed by k^{th} ant or the delay of finding a destination, or the available bandwidth of the link or the energy consumption of each node along the way and so on. Which parameters should be considered in the cost function depends on the concrete application.

```
procedure ACOMetaheuristic
    ScheduleActivities
        ConstructAntsSolutions
        UpdatePheromones
        DaemonActions           % optional
    end-ScheduleActivities
end-procedure
```

Listing 2.1: The ACO meta-heuristic in pseudo-code.

There are many other variations of ACO, the concrete equations applied for path search and pheromone update could be varied from the ones previously introduced in this section. However, the ACO algorithm can be generally described as the interplay of three procedures, as shown in listing 2.1 [17]. ConstructAntsSolutions is the procedure in which a colony of ants concurrently find the solutions in the construction graph. UpdatePheromones is the process in which ants modify the pheromone trails. DaemonActions is an optional procedure which is designed for implementing centralized actions. These three procedures conduct many researchers to design their own protocols.

The main merit of the ACO meta-heuristic is that it presents a common framework for approximating solutions to NP-hard optimization problems. Due to the dynamic nature of ACO's connectivity, ACO is able to continuously adapt to network changes in real time [18]. Moreover, the artificial ants can find multiple solutions simultaneously for the considered problem [17]. Therefore, it makes ACO specially applicable to dynamic problems, such as routing in telecommunication networks. Since the middle 1990s, the number of applications based on the ACO algorithms has bloomed. Until now, ACO algorithms have already been applied to solve routing problems in MANETs and WSNs with better scalability than other approaches.

2.2.3 Review of ACO-based routing protocols in MANETs

Since the end of 1990s, ant inspired algorithms have been applied to solve routing problems in network communications. By now, a great number of such approaches exists. In this section, some well-known ACO-based routing protocols for MANETs are presented. It includes not only the initial designs which aim at providing optimal routes, but also different approaches which consider special issues, such as QoS, energy reserves, location information and security during the route setup process. In order to give a better overview, theses protocols are categorized into five main directions based on the design purposes of the protocols. Figure 2.2 shows the categorization scheme in detail.

Basic ACO-based routing protocols

Initially, the optimization property of ACO algorithms has attracted much attention. Inspired by it, researchers have been motivated to apply ACO algorithms to find optimized routes for network communications. There are many approaches that belong to this category. In this subsection the most famous ones are introduced in chronological order.

AntNet G. Di Caro and M. Dorigo have proposed AntNet [51], which is the first representative ACO-based algorithm for solving the problem of internet routing. In AntNet, each node proactively sends out Forward ANT (FANT)s to discover a path to a randomly chosen destination node. Once FANTs reach the destination, Backward ANT (BANT)s are sent back to the source node following the reverse path. BANTs update the local models of the network status and the local routing table at each intermediate node. The performance of AntNet is evaluated in three different wired network scenarios.

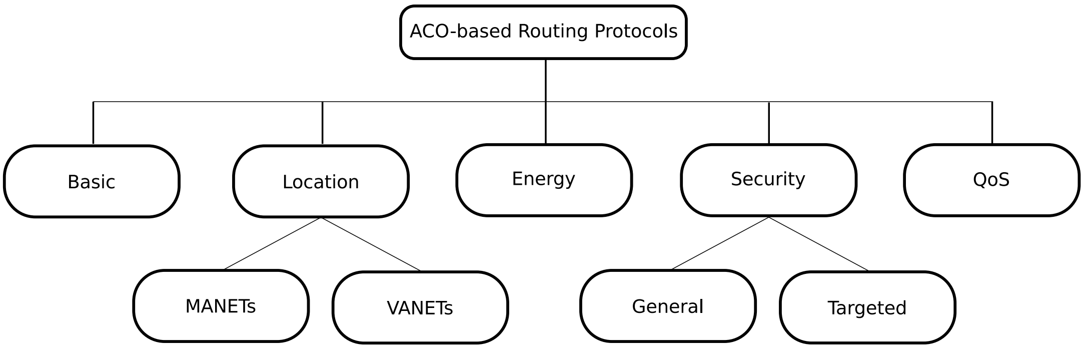


Figure 2.2: Types of ACO-based routing protocols in MANETs.

ARA Another representative ACO-based routing protocol for MANETs, ARA [52] was proposed by Günes et al.. ARA is an on-demand routing algorithm, which is based on a simple ant colony optimization meta-heuristic algorithm. The whole routing algorithm consists of three phases: a route discovery phase, a route maintenance and a route failure handling. The route discovery phase in ARA is designed in a similar way to AntNet. FANTs and BANTs are used in the route discovery phase. FANTs are broadcasted by the sender. Duplicate FANTs are identified by their sequence numbers and are deleted by intermediate nodes. Once FANTs reach their destination nodes, BANTs are created and sent back to the source nodes. Different from AntNet [51], ARA uses data packets to maintain the route to avoid the overhead caused by using periodic ants. If a node recognizes a link failure, it first sets the pheromone value of this link to zero to deactivate it. Then it searches for an alternative link. If this fails, it informs its neighbors. This process is repeated until an alternative route has been found or the source node receives a route error message. In the latter case, the source node will initiate a new route discovery phase if there are still packets to be sent.

PERA J. S. Baras and H. Mehta have proposed PERA, a proactive routing protocol [53]. PERA uses ant-like agents to discover the network topology and maintain routes in dynamic networks such as MANETs. PERA uses three kinds of ants: regular FANTs, uniform FANTs and BANTs. Regular and uniform FANTs are sent out proactively. These ants explore and reinforce available routes in the network. Uniform FANTs are routed in a different way than regular FANTs. Instead of using the routing table at each node, uniform FANTs choose the next hop node with uniform probability. Uniform FANTs help avoid that previously discovered paths become overloaded. BANTs are used to adjust the routing tables and statistic tables at each node, according to the information gathered by FANTs. The authors have compared PERA with AODV [8]. The results indicate that PERA has lower delay in all cases. However, the throughput of PERA at the higher speed is slightly less than AODV and the goodput of PERA is lower than AODV in high mobility scenarios.

AntHocNet Di Caro, Ducatelle and Gambardella have presented a hybrid multi-path routing algorithm, AntHocNet [54]. In AntHocNet there are six different kinds of ants: Proactive Forward ANT (PFANT)s, Proactive Backward ANT (PBANT)s, Reactive Forward ANT (RFANT)s, Reactive Backward ANT (RBANT)s, RePair Forward ANT (RPFANT)s and RePair Backward ANT (RPBANT)s. In the reactive route setup process, if a source node has no routing information about the requested destination node, it broadcasts RFANTs. Otherwise, it unicasts. When this RFANT reaches the destination, a RBANT is sent back to the source. Along its journey, the RBANT collects quality information about each link in the path and updates the pheromone table at each intermediate node. Once the first route is constructed, AntHocNet starts the proactive route maintenance process. Here, source nodes send out PFANTs to their destination nodes. PFANTs consider both regular and virtual pheromone for choosing the next hop node at each intermediate node.

Once a PFANT reaches the destination node, it is converted to a PBANT. PBANTs update the regular pheromone table on their way back to the source node. In case of a link failure, RPFANTs and RPBANTs are used to handle the problem. The authors have implemented the protocol in QualNet [55] and investigated its performance using various simulations and comparing the results to AODV [8].

PACONET E. Osagie et al. have proposed an improved ACO algorithm for routing called PACONET [56]. In PACONET, a source node reactively broadcasts FANTs in a restricted manner to explore the network. Each FANT records the total time it has traveled and maintains a list of all visited nodes. At each intermediate node the FANT updates the pheromone value. Once a FANT arrives at the destination, a corresponding BANT is generated. The BANT uses the list of visited nodes recorded by the FANT to travel back to the source node. Along the way, the BANT also updates the pheromone value in the reverse direction. Different from the AntNet, PACONET let both FANTs and BANTs update the pheromone. The performance of PACONET has been compared with AODV [8].The results show that PACONET has less end to end delay and routing control overhead than AODV, but the packet delivery ratio is nearly the same.

ACO-AHR W. Yu et al. have proposed a hybrid routing algorithm ACO-AHR [57], which includes reactive routing setup and proactive routing probe and maintenance. There are two kinds of agents: ant agents and service agents. The ant agent are FANTs and BANTs as in other ACO-based routing algorithms. In the reactive routing setup process, a source node broadcasts FANTs. Along the trip, each FANT records all the nodes it has visited in order to avoid cycles in the path. Each BANT carries all the information collected by the corresponding FANT. It calculates the delay from one intermediate node to the destination node. Once a BANT ant reaches the source node, a service agent is created. The service agent updates the routing table at intermediate nodes by using the information gathered by the BANT. In the proactive routing maintenance process, proactive FANTs are sent out while the data session is ongoing. The proactive FANTs are normally unicasted, but they could be broadcasted with a small probability. In the latter case, the FANTs may be able to find new paths.

HOPENT HOPENT is proposed by J. Wang et al. in [58]. It is based on the zone routing framework, combined with an ACO algorithm. HOPENT performs local proactive route discovery within a node's neighborhood and reactive communication between neighborhoods. HOPENT is simulated on GlomoSim [59] and the authors have compared HOPNET with several famous routing protocols, such as AODV [8], AntHocNet [54], and ZRP [60]. The results indicate that HOPNET is highly scalable for large networks in comparison with AntHocNet [54]. Moreover, the author also varied the zone radius in the experiments and results indicate that the selection of the zone radius has considerable effect on the performance.

Ant-E S. Sethi and S. K. Udgata have proposed an ACO-based on-demand routing protocol Ant-E [61]. Ant-E uses Blocking Expanding Ring Search (Blocking-ERS) [62] to limit overhead and controls local retransmission to improve PDR. The authors compared Ant-E with AODV [8] and DSR [9]. The results show that Ant-E performs better.

Summary In this section, some of the representative protocols which were proposed in the early stage of ACO-based routing protocols are introduced. The first ACO-based routing protocol, AntNet, proposed in 1998, gave a good example of how to apply the ACO algorithm in communication networks. In the following ten years, many subsequent researchers proposed various ACO-based routing protocols for MANETs based on this idea. Protocols in this category aimed for finding the optimal routes in dynamically changing networks and their performance indicated that ACO is a promising solution for routing problems in MANETs. This further encouraged researchers to design novel ACO-based routing protocols which consider other issues, such as QoS, energy consumption and so on.

QoS aware ACO-based routing protocols

QoS has always been a focus of attention in mobile ad hoc networks. It is a challenging problem when transmitting packets via multiple paths in a dynamic network. At the same time, the pheromone concept from ant colony algorithms also inspires many authors to use QoS parameters for selecting routes.

ARAMA ARAMA [63] is an early proactive routing algorithm proposed by O. Hussein and T. Saadawi. The FANTs in ARAMA gather both local and global path information, which could be the QoS parameters such as the remaining battery energy, delay, numbers of hops, etc. ARAMA defines a local normalized link index which is a good measure for overall path information. Once the FANT reaches the destination, the path grade is calculated based on this path index. A BANT follows the reverse path to the source node and updates the pheromone table at each hop.

SAMP-DSR SAMP-DSR [64] is proposed by E. Khosrowshahi-Asl et al., which aims to solve the shortcomings of both ACO and DSR [9] algorithms. In SAMP-DSR, each node can operate in two modes, called "local mode" and "global mode". Depending on the rate of network topology change, nodes switch between the two modes, in order to help the ants converge efficiently.

QAMR QAMR [65] is a QoS-enabled ant colony based multipath routing protocol for MANETs which is proposed by Krishna et al. It selects paths based on Next Hop Availability (NHA) and the path preference probability. The NHA is defined as the availability of nodes and links for routing on a path, considering both mobility and the energy factors. In order to find the best path that satisfying the QoS constraints, QAMR uses a path preference probability which measures different parameters such as delay, bandwidth and hop count. However, there are many extra control messages for estimating the quality of outgoing links.

QoRA A. Al-ani and J. Seitz have introduced QoS Routing protocol for multi-rate ad hoc networks based on Ant colony optimization (QoRA) [66]. In order to reduce the overhead when collecting information from multiple paths and to avoid congestion during data transmission, this paper uses Simple Network Management Protocol (SNMP) [67] to estimate QoS parameters locally. The proposed mechanism consists of two components: the QoRA entity and the SNMP entity. The QoRA entity runs on every node to identify a suitable route that meets the specified QoS requirements, while the SNMP entity collects detailed information about the characteristics of the outgoing links such as bandwidth, delay and packet loss. More specifically, the QoRA entity consists of five components: the neighbor table, the routing table, the ant Management, the decision engine and the QoS manager. while the two tables are common components of a routing protocols, the other three components are specially designed for QoRA. The ant management is responsible for generating FANTs, BANTs and Error ANT (EANT)s, all of which contain specific information necessary to provide QoS-aware routing and to identify pheromone deposits. The QoRA decision engine is a vital part which decides which of the different ants are to be sent and which updates the neighbor and routing table. The QoS manager acts as a command generator and notification receiver application. It also calculates QoS parameters locally based on communication with the SNMP entity. QoRA consists of five phases regarding route discovery and route maintenance. The first phase is the forward phase. The source node broadcasts a FANT to the network to find the best route to the destination. Before forwarding the packets, each intermediate node checks the Forward ANT Stack (FANTStack) to avoid loops and whether the given QoS requirements are satisfied. In the packet forwarding phase, intermediate nodes read the flow information and randomly forward the packets based on a probability roulette-wheel selection scheme [68] using the data in its routing table. The Backward phase starts after the destination node receives FANTs. The destination node calculates the residual QoS values and sends a BANT back to its neighbors. The BANT collects route quality information, refreshes the routing table, updates the pheromone and computes the QoS threshold. The Monitoring phase is mainly used for avoiding congestion problems by monitoring decreasing transmitting speeds. For each flow, QoRA communicates with the SNMP entity to calculate QoS parameters locally. If the required QoS is not satisfied in a certain period time (a monitoring window), the affected node broadcasts an EANT to inform the previous nodes about the congestion problem. When a node detects the loss of a link to a neighboring node, it deletes the information about this neighbor node from the neighbor table and updates the route table by finding an alternative path using EANTs. QoRA does not require either exchanging additional control packets or synchronizing nodes with the help of the SNMP entity. It computes QoS parameters locally to reduce overhead. The computation of QoS parameters is all loaded to the SNMP entity which allows QoRA to reduce end-to-end delay. Although it is clear that the QoRA entity requires less overhead, the communication between the QoRA entity and SNMP entities consumes more energy and bandwidth.

Summary In this section five representative protocols which focus on QoS fulfillment are discussed. QoS has always been a vital task for data transmission in MANETs. The approaches focus mainly on the parameters: link stability and hop count. Other common QoS related improvements are a reduction in overhead produced by control messages and the ability to eschew the requirement of time synchronization. Many other QoS parameters such as link delay, remaining battery energy, end to end reliability and bandwidth are treated as pheromone reinforce factors in above protocols.

Energy aware ACO-based routing protocols

In general, energy efficiency is one of the key parameters which should be considered while designing new routing protocols for wireless mobile networks and especially for WSNs. As shown before in section 2.2.3, some of the proposed ACO-based routing protocols for MANETs have used nodes' power reserves as a criterion in QoS computation. However, many conventional routing protocols suffer from sudden deaths of nodes in the network, because packets are always transmitted through the shortest paths. Therefore, nodes which participate in the shortest paths consume more power than other nodes. Network load imbalance leads to a reduction of network's lifetime. This problem recently has received more attention and many energy-efficient protocols which aim to extend network lifetime are proposed. The ACO-EEAODR [69] and Energy-Aware Ant based Routing (EAAR) [70] protocols are two earlier attempts in this direction.

ACO-EEAODR I. Woungang et al. [69] have improved an energy-efficient ad hoc on-demand routing protocol by embedding an ACO algorithm into it, calling the result ACO-EEAODR. It considers both the remaining battery power and the length of the path, while selecting the most energy-efficient path. There is a trade-off between the two parameters. Due to the priority of energy efficiency in this protocol, the weight of the first criterion is set to 0.7. Moreover, the updates of pheromone values in each node are also based on the remaining battery power. Therefore, an ant prefers hopping to a node with higher battery power rather than following the shortest path.

EAAR The EAAR [70] protocol is proposed by S. Misra et al.. In order to increase the battery life of a node, it considers both multi-path transmission and power consumption in forwarding a packet. The residual battery capacity is also considered in the proposed algorithm. The Maximum of the Minimum Residual Battery energy (MRB) of a route and the hop count are used to update the pheromone in the routing table during the route discovery phase. The results show that EAAR has the minimal energy consumption in the overall network and a low packets loss rate compared to AntHocNet [54]. However, the energy consumption per packet and the delivery rate are not as superior as the previous mentioned two parameters in high mobility scenarios. This is probably because EAAR needs more time to select the best route for data transmission.

AntHocMMP P. Vijayalakshmi et al. have proposed a robust energy efficient ACO routing algorithm named AntHocMMP [71], which uses ant agents to find optimal paths based on the Max-Min-Path (MMP) approach. The proposed algorithm first selects a set of relative paths from the source node to the destination by using the MMP algorithm. In the second phase FANTs are broadcast on all relative paths. While traversing along the relative paths, FANTs update the pheromone values at each intermediate node, to find the shortest and most robust path. Additional, AntHocMMP uses an adaptive re-transmission approach to detect link failure and select new relative paths. However, in the first phase the MMP algorithm has already traversed all the possible energy efficient paths from the source to destination and the pheromone deposits do not affect the selection of relative paths. Therefore, in this approach, the ACO algorithm is not used for finding possible paths, but for selecting the optimal path. This two procedure based approach is different from conventional ACO-based routing approaches.

ACECR J. Zhou et al. [72] have introduced the Ant Colony based Energy Control Routing (ACECR) protocol for MANETs. Different from the EAAR [70] which considers only the residual battery power of nodes, ACECR takes both the average energy and the minimum energy of a path into account, in order to select a path with more residual energy when considered from a global view. During the route discovery phase BANTs update not only the pheromone table by calculating the minimum and summing up of the nodes' residual energy values, but also the average energy of a path and hop count. The pheromone amount represents how good the path is to transmit a data packet. The authors have tested the protocol's performance with three different mobility models, namely the random walk mobility model, the Random WayPoint model (RWP) model [73] and reference point group mobility. All the simulation results show that ACECR has better performance than EAAR with respect to the data packet delivery ratio, routing load ratio, energy consumption of nodes and average end-to-end delay.

Hybrid ACO Recently, S. B. Prabaharan and R. Ponnusamy [74] have proposed a hybrid ACO routing protocol that emphasizes the security and energy efficiency. This protocol is abbreviated as Hybrid ACO from here on. In contrast to the conventional ACO routing protocols, this hybrid ACO routing approach selects the next hop node by using Simulated Annealing (SA). SA is a probabilistic approach which has a low probability of sinking into local optima. In the initial phase of the transmission, each link in the network is given a trust value as the initial pheromone value. Once the source node needs to discover a new route, it sends out FANTs. Before moving to the next hop, each FANT shortlists five neighboring nodes of the current node, marked with $L1$, using

SA. Each of the selected neighboring node shortlists five of its own neighboring nodes, marked with $L2$, also using SA. The best node of $L2$ is identified based on the trust values. Once the best $L2$ node is selected, the corresponding upstream node from $L1$ is also identified. Then the FANT moves to this identified node in $L1$. After each movement of the FANT, the trust values of all the links are updated. For links which the FANT hasn't visited, the trust values evaporate at a constant rate. The same methodology is repeated until the FANT arrives at the destination node or the maximum path length is reached. The novelty of this proposal is mainly that FANTs identify the next hop node by comparing trust values of 25 selected nodes in a two hop distance. Moreover, in order to find routes with minimal node reuse and to distribute the load through the network, this hybrid ACO routing protocol has incorporated randomness into the system to determine the paths. With the help of randomness during path selection, the energy depletion of certain centralized nodes is reduced. This enhances network stability further. However, the definitions of trust value related metrics, for example the stability, and the selection of the appropriate weight values for each metric are not clearly described.

Summary The energy reserve parameter used to be just one of many of QoS requirements, but in recent years it has become a popular topic in MANETs by itself. Repeatedly using the shortest path will drain the battery of the nodes on it, reducing their lifetime compared to other nodes. This will also decrease the lifetime of the network as a whole. The reviewed protocols in this section, all use the remaining battery power as a critical pheromone reinforcement factor to achieve high energy efficiency and extend the lifetime of the network. Another notable point is that most of the protocols in this section achieve lower energy consuming at the expense of the route discovery delay and the path length.

Location aware ACO-based routing protocols

With the utilization of the GPS [75], the location information of nodes becomes a popular issue when applying the routing protocols in practical. In this section six respective location aware ACO routing protocols are introduced in short. The survey paper [76] gives more details.

POSANT S. Kamali et al. [77] proposed an early reactive POSition based ANT colony routing protocol (POSANT) for MANETs. It combines the location information with traditional ACO routing algorithm, which aims to reduce the route establishment time while keeping less number of control messages. POSANT assumes that each node knows about its position, the position of its neighbors and the destination node. Then it uses the concept of zone which divides a node's neighborhood into three zones based on the physical location. For route discovery, the source node sends one FANT to each area on demand.

Robustness-ACO Unlike POSANT, D. Kadono et al. [78] have proposed a position aware ACO routing approach in MANETs which requires no location service. The proposed protocol is abbreviated as Robustness-ACO from here on. This paper constructs paths based on the robustness using the GPS information of visited nodes. The authors present two robustness functions to calculate the robustness value of a link. Based on this robustness value, the artificial ants decide the amount of pheromone to lay down. Each node predicts link disconnections by using the GPS information of its neighbors and redistributes the pheromone to accelerate alternative path construction. This mechanism is better adapted to dynamic network change and frequent link disconnection. The successful implementations of ACO-based routing protocol in MANETs [2] inspire the applications in VANETs [4]. VANET is a special type of MANETs which generally consists of a group of vehicles with a relatively high speed.

MAR-DYMO S. L. O. B. Correia et al. [79] have likely proposed the first ant-based algorithm that adapted to DYnamic MANETs On-demand routing protocol (DYMO) in vehicle ad hoc networks. The vehicles' information, such as speed and position, is applied to help updating the pheromone and making routing decision. Moreover, during the pheromone deposit process, MAR-DYMO uses Nakagami Fading Model [80] to indicate the path quality while utilizing Kinetic Graph framework [81] to show the link's stability. However, this mechanism consumes large amount of bandwidth and is not scalable [82]. The authors have simulated the vehicle mobility with the Vehicular Network Movement Generator (VNMG) [83] and implemented the proposed protocol in NS-2 simulator [84].

MAZACORNET In [82] H. Rana et al. introduce a hybrid ant based routing protocol for VANETs that first divides the networks into zones to achieve scalability. To reduce broadcasting and congestion, they use a proactive approach within the zones to find routes and a reactive approach between zones. In MAZACORNET, the pheromone deposition and evaporation model is the same as with MAR-DYMO [79]. The difference is MAZACORNET uses five types of ants to discover the route within or outside the zone, and two routing tables to maintain the routing information. However, this paper does not explain how zones could be formed in a fast dynamic VANET.

Cluster-based ACO Unlike the flat architecture of the zone-based hybrid ACO routing protocol, a hierarchical approach for VANETs is proposed by S. Balaji et al. [85]. It combines a clustering architecture with ACO routing procedures to enhance the scalability with a better organization for the network. This protocol is abbreviated as Cluster-based ACO from here on. To achieve an efficient management, this protocol firstly divides the network into multiple virtual clusters by broadcasting a MEmber Packet (MEP). After autonomous clustering, ACO-DYMO routing procedures are employed in the same way as in MAR-DYMO [79]. One notable idea in this protocol is that it uses a reactive approach instead of using a hybrid approach which is otherwise commonly applied in cluster-based networks.

S-AMCQ In recent year, M. H. Eiza et al. [86] have proposed a Secure Ant based Multi-Constrained QoS routing algorithm (S-AMCQ) for vehicle ad hoc networks, which considers not only QoS constraints, but also the security issues. In route discovery process, S-AMCQ applies ACO algorithm to explore numerous routes which satisfy multiple QoS constraints. And it uses an authentication mechanism to defend against external attackers. For the detection of internal attackers, S-AMCQ utilizes an extended VANET-oriented Evolving Graph (VoEG) model to perform plausibility checks on routing control messages. It also protects vehicles' privacy by using pseudonymous certificates. However, the authentication process in S-AMCQ is centralized and requires a Certification Authority (CA) that shows it is designed for Vehicle-to-Infrastructure (V2I) communications.

Summary The protocols introduced in this section represent a steady development of location aware ACO routing algorithms that leverage GPS. POSTAN [77] minimizes message delivery delay, while Robustness-ACO [78] combines robustness-based path construction with predictions of link disconnection. After the successful implementation in MANETs, many new ACO-based routing protocols are also designed for VANETs. MAR-DYMO [79] guarantees both link quality and stability. In order to improve the performance, researchers focus on modifying MAR-DYMO into two architectures, namely zone-based and cluster-based architectures. MAZACORNET [82] subdivides the networks into zones to achieve scalability. A proactive approach is used within the zones while a reactive approach is applied between zones. Different from MAZACORNET, Cluster-based ACO [85] aims to reduce the number of routing control packets. However, message delivery in the network after the autonomous clustering is not described. S-AMCQ [86] considers both the QoS constraints and the security issues to ensure reliable and robust routing in VANETs. In general, location aware ACO routing protocol have been well developed and show good prospects.

Security aware ACO-based routing protocols

Other than QoS and energy efficiency, security is another hot topic in routing protocols which attracts many researchers' attention. As is well-known there exist many security threats in the network layer, such as black hole attacks, wormhole attacks, flooding attacks and so on. When these attacks are launched during the routing process, this usually leads to strong harmful effects on the network. In the worst cases, an attacker might even make the communication in the network impossible. Therefore, mechanisms that helps participants in a network to defend against the potential attacks are necessary. However, the scope of security is wide. Different researchers have their own ideas about how to best build defense systems. In this section, an overview about existing security aware ACO-based routing protocols is presented.

SAR-ECC V. Vijayalakshmi and T.G. Palanivelu [87] have proposed a secure ant based routing algorithm for cluster based ad hoc networks using Elliptic Curve Cryptography (ECC) [88], which is abbreviated as SAR-ECC from here on. This approach makes use of two basic processes: one is estimating the trust value between neighbor nodes. The other uses the AntNet routing mechanism for route discovery and ECC for mutual authentication between the source and destination. In the network, each node in the cluster keeps trust values for all its neighbors. A trust value is calculated based on a measurement of uncertainty and is an increasing function that correlates with the probability of successfully transmitting each packet. During route establishment, the source node tries to find multiple routes using AntNet [51]. Then it gathers the trust values of all nodes in the paths. Based on the trustworthiness of nodes, it selects a trustworthy route for data transmission. The novelty of the protocol is using a trust value based on a measurement of uncertainty instead of the conventional pheromone. However, the updating mechanism for the trust value is not described and the benefits of combining a cluster structure with an ACO algorithm is not clearly described.

SPA-ARA Secure Power-Aware Ant Routing Algorithm (SPA-ARA) inspired by ACO algorithms is proposed by S.Mehfuz and M.N.Doja [89]. SPA-ARA aims to not only manage energy usage, but also to guarantee security in MANETs. Similar to other ACO-based routing protocols, SPA-ARA also launches ants to explore the network. Once a source node needs to send data packets to one destination node, it checks its pheromone table first. If there exists route information, it chooses the corresponding node as the next hop for which the next-hop availability is maximum. Afterwards, data packets secured by a Message Authentication Code (MAC) are transmitted along stochastically chosen routes by using the pheromone tables along the whole route. If there is no route information about the particular destination, the source node sends out reactive FANTs. These reactive FANTs are also attached with the MAC, which is generated using the HMAC keyed hash algorithm [90] with a shared group key. After receiving the reactive FANTs, intermediate nodes check first whether the attached MAC is valid. If it is correct, the intermediate node determines the trust value of the previous hop by looking it up in own trust pheromone table. Only if this trust value is above a predefined threshold value, the intermediate node accepts the FANT and establishes a secret key with the previous hop node by using a two-party key establishment protocol. This secret key is used for verifying the BANT later. As a consequence, a secret key is set up between each pair of neighboring nodes along the route. Once the destination node receives the FANT, it reacts analogously to the intermediate nodes. Only if the FANT has a valid MAC and the trust value of the previous hop is above the threshold, the destination node generates a corresponding BANT. Otherwise, it discards the FANT without taking any further action. This BANT is secured with a MAC generated with the secret key between the destination node and the next hop in the path towards the source node. Intermediate nodes verify the MAC attached to the BANT by using the corresponding secret keys hop by hop. When the BANT successfully arrives the source node, it has also updated all the pheromone tables along its journey. Based on the attached MACs and pairwise secret keys, the ants finish the authentication process in the reactive path setup phase. The authors have written that SPA-ARA could protect the network from most common attacks on routing protocols for ad hoc networks and have compared its performance with the Source Routing Protocol (SRP) [91] protocol. The results show that SPA-ARA has longer lifetime than SRP, and attackers lead to less dropped packets in SPA-ARA. In order to maximize network lifetime, the number of hops, travel time and the batteries' remaining energy are chosen as the optimization parameters, which directly affect the pheromone updating process. Going from these results, SPA-ARA has the lowest energy level standard deviation when compared to the AODV [8], DSR [9] and ARA [52] protocols. It also discovers the most successful routes. The proposed scheme pays attention not only to security, but also to the nodes' remaining energy so as to achieve a fair distribution of energy usage. Due to the cryptographic mechanism frequently used in the MAC and when broadcasting FANTs in the route discovery phase, overhead is one of most critical parameters for evaluating the performance of the proposed routing protocol. However, the authors haven't shown any results regarding overhead.

FTAR Fuzzy logic has been widely utilized in many areas of the daily life. Since the 1980s, many fuzzy logic based systems have been proposed in many fields, such as automatic control, automobile production, academic education, industrial manufacturing and so on [**?**]. Due to its great success, researchers [92], [93], [94], [95] have designed new routing protocols in MANETs, combining fuzzy logic with ACO algorithms. S. Sethi and S. K. Udgata [96] have proposed the Fuzzy-based Trusted Ant Routing (FTAR) protocol in 2011. FTAR combines swarm intelligence and the fuzzy system to select the optimal path. In the route discovery phase, it follows the same concepts as those used in many other conventional ACO routing protocols. FANTs travel through the network hop by hop using Blocking-ERS [62]. In order to prevent cycles in the path, each intermediate node stores recently forwarded route requests in a buffer. BANTs travel back along the routes of their corresponding FANTs until they reach the source node. After pheromone

© 2017 IEEE

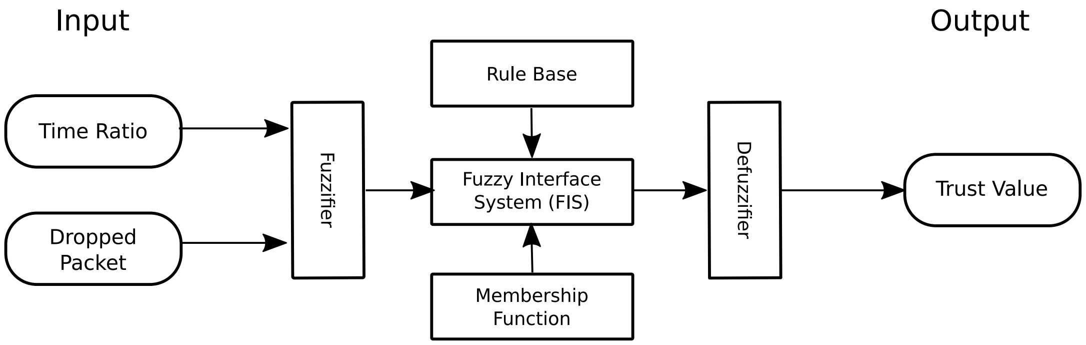


Figure 2.3: Fuzzy system for trusted node.

tracks are established between source and destination nodes, data packets update the pheromone values along the path while they are transmitted to the destination node. If there is no data communication in the network, pheromone values evaporate with the time. If a node does not receive an acknowledgment within predefined interval, it generates a route error message and the pheromone value of the related routes reduce to 0. Meanwhile, the node tries to deliver the data packet to the destination via alternative routes. FTAR aims to distinguish between healthy and malicious nodes, and has introduced a fuzzy-based trusted node model. In this model each node is assigned a trust value signifying its trustfulness. As shown in figure 2.3, input parameters for the fuzzy control are chosen to be the dropped packets and time ratio, which represents the ratio between the route reply time and the time-to-live. The membership functions of the two input and single output parameters are assumed to be Gaussian functions. Each input parameter is categorized into four levels; and the output parameter is appraised by five levels. A series of rules are defined for the Fuzzy Inference System (FIS). Smallest Of Minimum (SOM) is applied for the defuzzification process. After the fuzzy process, the fuzzy trust value is evaluated. It can affect the route discover phase, because FANTs only choose trusted neighbor nodes on their paths. In the presence of unsafe or malicious nodes, the results show an improvement over the Ant-U algorithm. However, the authors neither explain how they obtain the input parameters for their fuzzy control system, nor do they give a detailed explanation of how to use the fuzzy based trust value in the ACO routing structure. Due to these reasons, FTAR is not re-implemented in this thesis. Moreover, the authors compared FTAR only with an algorithm called "Ant-U" which was not introduced in the paper or anywhere else. The lack of comparison between FTAR and other security aware routing protocols or even regular state of the art routing protocols reduces the usefulness of their evaluation and makes their results hard to appreciate.

SBDT G. Indirani and K. Selvakumar [97] have proposed Swarm Based intrusion detection and Detection Technique (SBDT) in 2012. It uses the swarm intelligence of ant colony optimization to establish multiple paths between source and destination nodes. Nodes with high trust values, residual bandwidth and energy are selected as Node Active (NA)s. Each NA monitors its neighbor nodes and collects all their trust values. NAs also exchange the gathered trust values with their neighbor NAs. If a node's trust value is below a predefined minimum trust value, the NAs mark it as malicious. Upon detecting a malicious node, the NA node informs a transmission's source node about the detection. In order to defend against the malicious node, the source node performs a key revocation process. In this approach, the trust value is a core factor to support the whole detection system. However, the authors haven't mentioned how the trust values are estimated and updated.

DBA-ACO Other than designing intrusion detection systems, researchers are also interested in preventing certain attacks. K. S. Sowmya et al. [98] have proposed an idea to prevent black hole attacks using the ACO routing structure, which is abbreviated as DBA-ACO from here on. The approach follows the conventional ACO routing protocols to discover routes. In order to detect black hole node, a dynamically updated threshold value is used. The threshold value is the average difference of the destination sequence numbers in the routing table and those brought back by the BANTs. If a BANT brings back a destination sequence number which is higher than the threshold value, the node who forwards this BANT is then considered a black hole node. Once a black hole node is detected, alarm packets with the black hole node's ID are distributed through the network. Hence, the nodes of the network can isolate the malicious node. This approach avoids the usage of any cryptographic mechanisms to ensure security in the routing protocol. However, the authors have not performed any simulation to test the performance of the proposed idea.

ANTNET S. Pal et al. [99] have found another way of detecting black hole attacks. They apply ACO to the AODV [8] routing mechanism, calling it ANTNET. This protocol first uses AODV to gather paths and then applies the ANTNET algorithm to detect the anomalies. Finally, it uses the ACO mechanism to rediscover paths. However, the update mechanism of the pheromone is not mentioned and there is no description about the concrete reactions after detecting the black hole nodes.

ABPKM P. Memarmoshrefi et al. have proposed [100] Autonomous Bio-inspired Public Key Management (ABPKM) approached for MANETs to defend against network layer attacks. The main idea is to apply ACO for self-organized public key management to prevent nodes' misbehavior and ensure the correctness of the public keys. The trust value in this approach is estimated based on identity assurance, which means the level at which the public key being presented can be trusted to represent a particular node and not some other nodes in the network. In order to combine the trust based public key mechanism with an ACO algorithm, the authors use the trust value as the pheromone value in the ACO algorithm. The proposed approach consists of four main parts: the initialization phase and certificate issuing, the certificate chain discovery, the public key authentication by certificate verification and the certificate chain trust/pheromone update. In first phase, public key certificates are issued by each node to its neighboring nodes upon receiving the corresponding public keys and the initial trust/pheromone value to all issued certificates are set with the threshold value 0.5. Once a source node wants to authenticate the public key of a destination node, the source node sends out FANTs to find desired certificate chains from the source node to the destination node. The route discovery process is similar to that of conventional ACO routing protocols, except the BANTs also carry certificate chains. After the source node has found the certificate chains, it needs to authenticate the public key represented by those chains. It retrieves the public key of the destination node from the received chains and computes the corresponding trust values of the chains. The route represented by the chain with highest trust value is chosen for data transmission. Based on the results of the public key authentication process, the source node updates the trust values of its neighboring nodes. The updating is launched hop by hop along the chains. Nodes in a chain without any fake certificate are rewarded with increasing trust values. In contrast, nodes in a chain which includes fake certificates are punished by their upstream nodes. In this paper, the authors have investigated the scalability and robustness of ABPKM by varying network size, mobility and the percentage of malicious nodes. The simulation results show that ABPKM provides good performance over a wide range of scenarios and remains stable for all tested network sizes. The novelty in this protocol is connecting the trust value from public key management with the pheromone in ACO algorithms. This design lets ABPKM reap benefits from both sides. After their first design, the authors have improved the model in [101] to detect more complex attacks, such as Sybil attacks, during the public key authentication phase. They add the agglomerative hierarchical clustering algorithm to ABPKM and analyze the nodes' behavior with a new Sybil attack detection model. Based on the gathered certificate chains, the source node extracts node features, such as the number of groups one node belongs to, the distance of a node to the destination node, the social degree of one node and the average trust value for the chains in which the node participates. These features help the source node to group other nodes during the clustering process. Another interesting parameter which is inspired from mate and non-mate discrimination in real ant colonies, the aggression value, is also newly introduced in the model. This value is used to estimate the danger level of one node in the network. After the clustering process, the node's aggression values are estimated. In their following work [102], they give additional simulation results. These show, based on an experimentally determined best cutoff point and aggression threshold values respectively for different network sizes, that moving nodes have a generally better accuracy for detecting the attacker nodes. However, these results are from the learning phase of the ACO-based autonomous authentication model. The performance of a complete routing protocol including the proposed detection mechanisms still needs to be investigated.

Summary This section has surveyed some of the existing security aware ACO-based routing protocols in chronological order. Based on the aims of these protocols, they can be divided into two groups: general and targeted, as shown in figure 2.2. The first group aims to generally detect anomalies in the network, while the other one targets a particular attack (e.g. black hole attacks). If only looking at the security model applied in these protocols, 71 % of them are trust based models. There are different ways to set up trust models. S. Sethi and S. K. Udgata [96] have applied the fuzzy logic to estimate the trust values in their protocol FTAR, while the other researchers [87], [89], [100] have applied authentication mechanisms to create their own trust models. From the observations, it shows that the combination of fuzzy logic and ACO could be well suited to improving the security in MANETs. However, choosing suitable parameters which should be considered in the fuzzy system is very important in order to estimate accurate trust values. The choice may be strongly influenced by the design aims of the protocol and also related to the experiences obtained by the designer. For example, the rule base which is used within a fuzzy system is usually made by experience and it can strongly affect the output results. More research which explores or discusses these open issues in this area are needed. Authentication mechanisms are an important feature used to improve the security in wireless networks. 80 % of the trust based models in this section have applied such mechanism. SPA-ARA [89] is one representative example of an authentication based approach in this section. The authors have pointed out that SPA-ARA can detect most of the common attacks in MANETs. However, due to the cryptographic mechanism frequently used for authentication, overhead is one of the most critical parameters for evaluating the performance of the proposed routing protocols.

Other ACO-based routing protocols

Instead of focusing only on a single issue such as QoS, energy, security, etc., researchers have also proposed other ACO-based routing protocols which consider two or more issues in the same time. In previous sections some of them are already reviewed. For instance, SPA-ARA [89], introduced in section 2.2.3, considers both energy and security in the routing process. Another example is S-AMCQ [86] in section 2.2.3, which considers the QoS and security in VANETs communication. Considering multiple issues in a routing protocol's design can make the protocol more suitable for real world applications. However, this is a new direction that has not been investigated by many researchers yet. Therefore, they are not categorized into a separate group. However, designing ACO routing protocols based on the multiple existing issues in MANETs and especially in VANETs, would be an interesting future research direction.

2.2.4 Analytical comparison of ACO-based routing protocols for MANETs

In this section the previously surveyed ACO-based routing protocols, which cover the time from 1998 to 2016, are summarized and compared based on the design patterns of these ACO-based routing protocols. Ten tables in this section show an analytical comparison of all the protocols according to the categories introduced in the previous section: basic optimization, QoS awareness, location awareness, energy awareness and security awareness.

Analytical parameters

The following seven parameters are chosen to compare the different ACO-based routing protocols:

Design goals: This parameter explains the aims of the proposed protocols. The goals usually indicate the categories which the routing protocol belongs to.

Ant types: In conventional ACO-based routing protocols, there are usually two types of ants: FANTs and BANTs. However, depending on the design of the protocols, there could be other types of ants in the network. This parameter lists all types of ants in the protocol.

Pheromone reinforcement factors (Ph. reinforcement): Pheromone is one of the most important parts in ACO-based routing protocols. This parameter specifies what is considered while reinforcing the pheromone values in the algorithm.

Table 2.1: Design parameter overview of basic ACO-based routing protocols

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
AntNet [51]	proactive	unicast	BANTs
ARA [52]	reactive	broadcast	FANTs, BANTs, DPs
PERA [53]	proactive	unicast	BANTs
AntHocNet [54]	hybrid	both	RBANTs, PBANTs
PACONET [56]	hybrid	broadcast	FANTs, BANTs
ACO-AHR [57]	hybrid	both	service agents
HOPENT [58]	hybrid	unicast	FANTs, BANTs
Ant-E [61]	reactive	broadcast	FANTs, BANTs, DPs

Table 2.2: Pheromone parameter overview of basic ACO-based routing protocols

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
AntNet [51]	distributed, robust, multi-path routing	FANT, BANT	goodness of trip time	goodness of trip time
ARA [52]	reduce overhead	FANT, BANT	hop count	constant rate
PERA [53]	reduce overhead	FANT, BANT, uniform FANT	delay, hop count, trip time	delay, hop count, trip time
AntHocNet [54]	efficient routing	PFANT, PBANT, RFANT, RBANT, RPFANT, RPBANT	hop count, delay	constant rate
PACONET [56]	efficient dynamic routing	FANT, BANT	travel time, run time parameter	constant rate
ACO-AHR [57]	apply multi-agents to reduce expense	FANT, BANT	travel time, ant release ration	constant rate
HOPENT [58]	high scalability, less overhead	IFANT,EFANT, BANT,NANT,EANT	travel time	constant rate
Ant-E [61]	control overhead, improve reliability	FANT, BANT	hop count	constant rate

Pheromone evaporation factors (Ph. evaporation): In ant colonies pheromone evaporates over time [17]. This allows ants to forget old paths. This parameter specifies what is considered while evaporating the pheromone values in the algorithm.

Routing approach: This parameter signifies if the routing protocol is proactive, reactive or hybrid.

Transmission type of FANTs (Tran. Type FANTs): This parameter explains the type of transmission for FANTs. The types used in all reviewed protocols in this work are unicast and broadcast.

Pheromone update activators (Ph. Activators): Pheromone in ACO-based routing protocols changes dynamically. This parameter explains where the pheromone is updated in the routing protocol.

The parameters mentioned before are divided into two groups, for example, as shown in table 2.1 and Table 2.2: the common basic design properties and the pheromone related core design properties. The first group introduces the basic routing structure, while the other group reflects the core ACO mechanism within the routing protocol. In the following subsections, results are presented in the form of these two kinds of comparison tables, dividing up the algorithms according to five categories that are previously introduced. In addition, each section's results are summarized.

Comparison of basic ACO-based routing protocols

Table 2.1 summarizes various basic optimization ACO-based routing protocols for MANETs. Many of them are representative algorithms in this category, such as AntNet [51], ARA [52], etc. Routing protocols could be classified into proactive, reactive and hybrid approaches, which is listed in the path establishment column. Overall, $75\,\%$ of the studied protocols in this category have a reactive or hybrid routing design, instead of using a proactive design, which usually causes more overhead for maintaining routing tables. This trend reflects the requirements of ad hoc network. Generally speaking, broadcasting a message produces more control messages, because the message needs to be transferred to all recipients simultaneously. On the contrary, using unicast method the message is sent to exactly one destination device. However, it has a relatively lower probability of finding global optima. $37.5\,\%$ of the reviewed protocols broadcast FANTs and another $37.5\,\%$ prefer unicasting them. It is also noteworthy that the remaining protocols, namely AntHocNet [54] and ACO-AHR [57], switch between unicast and broadcast type, based on whether there is any routing information about destination nodes. A less common way of updating pheromone values is presented in ARA [52] and Ant-E [61] where data packets update the pheromone and in ACO-AHR [57], where service agents take over this duty.

After having an overview of the common design properties, the properties of the pheromone applied in these ACO-based routing protocols are introduced. Table 2.2 includes some representative ACO algorithm related parameters: design goals, ant types, the pheromone reinforcement factor(s) and the pheromone evaporation factor(s). The basic optimization routing protocols in Table 2.2 aim to efficiently find optimal routes with limited routing overhead. Most of the studied protocols use two kinds of ants, FANTs and BANTs. Due to different requirements in the reactive and proactive routing phases, many hybrid protocols use more than two types of ants. For example, in HOPNET [58]. The way in which pheromone values are calculated differs among the listed protocols. The metrics used for reinforcing the pheromone are usually hop count, ant's travel time, end to end delay and path goodness. Most of the protocols consider a combination of these metrics with separate weights, according to the requirements of the corresponding protocol. The pheromone evaporation process is based on evaporation factors which can be dynamic or static. The common evaporation factor is a predefined constant rate. One example of the dynamic evaporation factor is the goodness of trip time factor used in AntNet [51].

Table 2.3: Design parameter overview of QoS aware ACO-based routing protocols

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
ARAMA [63]	proactive	unicast	BANTs
SAMP-DSR [64]	hybrid	unicast	RREQs
QAMR [65]	reactive	broadcast	BANTs, FANTs
QoRA [66]	reactive	broadcast	BANTs

Table 2.4: Pheromone parameter overview of QoS aware ACO-based routing protocols

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
ARAMA [63]	Optimize hop counts and QoS, energy efficient	FANT, BANT	queue delay, remaining battery energy, link's signal to noise ratio, bit error, path grade	path grade
SAMP-DSR [64]	Solve the shortcoming of ACO and DSR	FANT, RREQ	end to end reliability, the trip time	unknown
QAMR [65]	Achieve link stability	FANT, BANT	bandwidth, delay, hop count	constant
QoRA [66]	less further control messages or without synchronization	FANT, BANT, EANT	constant	constant

Comparison of QoS aware ACO-based routing protocols

Quality of Service is the primary mission for data transmission and communication in MANETs. Table 2.3 presents the basic properties of the selected four QoS aware ACO-based routing protocols. Similar to the result from Table 2.1, 75 % of the studied protocols in this section have designed the protocol with a reactive or hybrid structure. ARAMA [63] as an early protocol is a proactive approach and SAMP-DSR [64] is a hybrid protocol. The recent protocols prefer to use reactive approaches such as QAMR [65] and QoRA [66], because they adapt better to real-time communications. The rest of table shows that half of the protocols broadcast FANTs while the other half unicast them. Only QAMR uses both FANTs and BANTs to update the pheromone while the others use just BANTs or RREQs, which are Route REQuest packets.

As shown in table 2.4, all the surveyed protocols aim mainly to ensure link stability and optimize hop count. QoRA attempts to reduce overhead produced by control messages or without synchronization. Parameters related to QoS such as delay, remaining battery energy, end to end reliability and bandwidth are considered as pheromone reinforcement factors in these protocols. Most of the reviewed protocols in this subsection use a constant rate to evaporate the pheromone except ARAMA which estimates the path grade and uses it as an evaporation factor.

Table 2.5: Design parameter overview of energy aware ACO-based routing protocols

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
ACO-EEAODR [69]	reactive	broadcast	RREPs
EAAR [70]	reactive	broadcast	BANTs
AntHocMMP [71]	proactive	unicast	FANTs, BANTs
ACECR [72]	proactive	broadcast	BANTs
Hybrid ACO [74]	reactive	unicast	FANTs

Table 2.6: Pheromone parameter overview of energy aware ACO-based routing protocols

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
ACO-EEAODR [69]	increase network lifetime	Route REQuest (RREQ), Route REPly (RREP)	remaining battery power	unknown
EAAR [70]	less energy consumption, multi-path transmission	FANT, BANT	MBR, hop count	constant rate
AntHocMMP [71]	path robustness, extend network lifetime	FANT, BANT	energy path cost	constant rate
ACECR [72]	extend network lifetime	FANT, BANT	avg. & min. energy, hop count	constant rate
Hybrid ACO [74]	secure, energy efficiency	FANT	predefined constant	constant rate

Comparison of energy aware ACO-based routing protocols

The limited battery power of nodes in ad hoc networks is one critical issue. Repeatedly using the shortest path will drain the battery of the nodes on it and decrease the lifetime of the network as a whole. For this reason energy efficiency has become a hot issue in designing routing protocols rather than being just one of many QoS requirements. Table 2.5 and 2.6 present the details of the comparison in this area.

Table 2.5 shows that only 40 % of the protocols set up routes proactively. While BANTs are usually unicast from the destination back to the source, FANTs are either broadcast or unicasted hop by hop. 60 % of the reviewed protocols in this subsection update pheromone after ants have reached their destinations. The concrete pheromone update activators in these protocols are either BANTs or RREPs. Besides BANTs, AntHocMMP [71] also uses FANTs to update pheromone values. Hybrid ACO doesn't specify the type of ants it uses. Pheromone updates occur before ants have reached the destination nodes. Therefore, it's similar to the protocols which use FANTs as the pheromone update activators. Table 2.6 shows that the main purpose of all energy efficient protocols is to extend the whole network's lifetime by reducing repetitive use of the same nodes in shortest paths. For pheromone reinforcement, Hybrid ACO just uses a predefined constant amount, while ACO-EEAODR [69] considers only the remaining battery power for updating pheromone values. ACECR [72] considers both the average energy and minimum energy of a path

Table 2.7: Design parameter overview of location aware ACO-based routing protocols

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
POSANT [77]	reactive	unicast	BANTs
Robustness-ACO [78]	hybrid	broadcast	FANTs,BANTs
MAR-DYMO [79]	reactive	broadcast	RREPs
MAZACORNET [82]	hybrid	unicast	unknown
Cluster-based ACO [85]	reactive	broadcast	RREPs
S-AMCQ [86]	reactive	unicast or broadcast	RQANTs

Table 2.8: Pheromone parameter overview of location aware ACO-based routing protocols

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
POSANT [77]	Min. delivery delay	FANT,BANT	distance,location	constant rate
Robustness-ACO [78]	construct robust paths	Hybrid FANT/ BANT	robustness,cost	constant rate
MAR-DYMO [79]	adapt ACO to VANETs	Hello message, RREQ/RREP	reception probability, lifetime ratio	path lifetime
MAZA-CORNET [82]	scalability,robust to link failures	Internal Forward ANT (IFANT),EFANT, BANT,Notification ANT (NANT), EANT	same with MAR-DYMO	same with MAR-DYMO
Cluster-based ACO [85]	improve MAC layer efficiency	Hello message, RREQ/RREP	same with MAR-DYMO	same with MAR-DYMO
S-AMCQ [86]	ensure reliable, robust routing	RQANT,RPANT REANT	QoS metrics, reliability value	individual variable

to select a path with more residual energy on a global view. Both EAAR [70] and AntHocMMP consider the Maximum of MRB of all nodes in a path. The difference between them is that EAAR uses MRB as a pheromone reinforce factor while AntHocMMP uses it to find relative paths.

Comparison of location based ACO-based routing protocols

In this subsection, the different parameters for the location aware ACO routing protocols are presented in table 2.7 and 2.8.

Table 2.7 shows that all the reviewed protocols avoid to apply the proactive approach, due to the overhead caused by proactively maintaining of routing tables. As for the transmission type of FANTs, ca. 50 % of all approaches broadcast FANTs while the remaining protocols except S-AMCQ, unicast FANTs. S-AMCQ broadcasts the routing control ants only when there is insufficient information available at the pheromone table. In the pheromone update phase, only in the Robustness-ACO protocol both FANTs and BANTs can update the pheromone. Utilizing the location information from GPS helps ACO-based routing protocols adapt better to MANETs, especially to VANETs. The main goals of many reviewed protocols in this subsection are to minimize delivery delay and establish robust routes. Various ant types are used in these approaches. Other than the basic FANTs and BANTs, there are IFANTs, External Forward ANT (EFANT)s, NANTs

Table 2.9: Design parameter overview of security aware ACO-based routing protocols

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
SAR-ECC [87]	reactive	unicast	unknown
SPA-ARA [89]	reactive	both	BANTs
FTAR [96]	reactive	broadcast	FANTs
SBDT [97]	reactive	unknown	unknown
DBA-ACO [98]	reactive	unknown	unknown
ANTNET [99]	reactive	unknown	ANTs
ABPKM [100]	reactive	unicast	BANTs

Table 2.10: Pheromone parameter overview of security aware ACO-based routing protocols

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
SAR-ECC [87]	secure routing	FANT, BANT	trust value	unknown
SPA-ARA [89]	energy efficiency, detect malicious nodes	FANT, BANT	distance, traveling time	constant rate
FTAR [96]	trusted routing	FANT, BANT	constant rate	constant rate
SBDT [97]	detect malicious nodes	FANT, BANT	unknown	unknown
DBA-ACO [98]	detect and prevent black hole attack	FANT, BANT	unknown	unknown
ANTNET [99]	detect and prevent black hole attack	ANT	trails, attractiveness	unknown
ABPKM [100]	secure self-organized authentication routing	FANT, BANT, RANT, UANT	trust value	constant rate

and EANTs in protocols which are designed for hierarchical networks, such as MAZACORNET. In some of the reviewed protocols, RREQs and RREPs are also used in the route discovery phase. Hop count and the cost of a route are two main pheromone reinforce factors in MANETs. In VANETs, however, this can be quite different due to frequent interruptions of paths. [79], [82], [85] in the VANETs scope use the probability of reception of a message, the ratio between the estimated lifetime of a path and the maximum allowed lifetime of a path, to update the pheromone. The protocols in MANETs use a constant rate for pheromone evaporation, while the VANETs protocols use the lifetime of a path or an individual variable value [86] to reduce the pheromone values.

Comparison of security aware ACO-based routing protocols

Due to the prevalence of security threats in the networks, security is also a hot topic that attracts many researchers' attention. Common attack types are, for example, black hole and wormhole attacks. Different researchers have proposed various ideas about how to ensure security in their routing protocols. In this section, a selection of security aware ACO-based routing protocols are compared. These protocols use several methods to ensure secure routing. Table 2.9 shows that all surveyed protocols in this subsection use reactive approaches, thus avoiding the higher overhead commonly associated with proactive methods. For example, besides the regular proactive routing table maintenance, if a malicious node is detected in proactive approaches, all nodes in the network need to put the malicious node into black lists and update their routing tables to avoid routes including the reported malicious node. Table 2.10 shows that most of the security aware ACO routing protocols aim to ensure finding secure and reliable routes. Some of them such as DBA-ACO [98] and ANTNET [99] focus on defending against certain attack types, while others are interested in detecting malicious or anomalous nodes in the network. All the listed protocols use the basic ant types, except ABPKM [100] which has two other special ant types, namely Repair ANT (RANT)s and Update ANT (UANT)s. Although some of the proposed protocols have not described their pheromone related parameters clearly, it still can be found that there are various pheromone reinforcement factors, which are applied in this subsection. Besides a trust value, which is the most common parameter, there are also other parameters used for reinforcing the pheromone values, such as traveling time, distance, trails and attractiveness. In contrast to the reinforcement factors, most of the protocols use a constant rate to evaporate the pheromone over time.

2.2.5 Simulation parameter comparison of ACO-based routing protocols

Comparison of implementation related metrics

Table 2.11 shows the representative performance metrics of the surveyed protocols in the five main categories. As can be seen in table 2.11, nearly 97 % of the surveyed protocols have implemented their ideas and evaluated their performance of these, ca. 83 % are implemented in common simulators, such as NS-2 [84], GloMoSim [59]/ QualNet [55], OMNet++ [104] and so on. Around 10 % protocols are implemented in self-developed simulators. Around 83 % of the studied protocols have compared their performance to that of other standard routing protocols for MANETs. AODV [8] is one of the most popular protocols chosen for comparison in earlier publications. After being presented to the public, AntHocNet [54] also becomes a benchmark ACO routing protocol commonly used for comparison.

In order to evaluate the performance, researchers mainly focus on Data Delivery Ratio (DDR), the end to end delay and the routing overhead. 80 % of the studied protocols have shown results for at least one of these three metrics. Moreover, nearly 79 % of the protocols in the basic and location aware ACO routing categories have evaluated all these three metrics. In the location aware ACO routing category this value even rises to 100 %. Meanwhile, the percentage of protocols which don't consider any special performance metrics in these two categories are 50 % and 40 % respectively. In the other three categories these values are much lower. This indicates that basic and location

Table 2.11: Simulation parameter overview of ACO-based routing protocols

	Protocol	Compare with	Simulator	DDR	Delay	Overhead	Special
Basic	AntNet [51]	OSPF,SPF,BF, Q-R,PQ-R, Daemon	own simulator [51]	NO	YES	YES	YES
	ARA [52]	AODV, DSDV,DSR	NS-2 [84]	YES	NO	YES	NO
	PERA [53]	AODV	NS-2	NO	YES	NO	YES
	AntHocNet [54]	AODV	QualNet [55]	YES	YES	YES	YES
	PACONET [56]	AODV	GloMoSim [59]	YES	YES	YES	NO
	ACO-AHR [57]	AODV	NS-2	YES	YES	YES	NO
	HOPENT [58]	AODV,ZRP, AntHocNet	GloMoSim	YES	YES	YES	YES
	Ant-E [61]	AODV,ZRP, AntHocNet	NS-2	YES	YES	YES	NO
QoS aware	ARAMA [63]	without	OPNET [103]	YES	NO	NO	YES
	SAMP-DSR [64]	EMP-DSR,MP-DSR, AODV,AntHocNet	OMNet++ [104]	YES	YES	YES	NO
	QAMR [65]	AODV, ARMAN	NS-2	YES	NO	YES	YES
	QoRA [66]	AODV, CLWPR	NS-3 [105]	YES	YES	NO	YES
Energy aware	ACO-EEAODR [69]	EEAODR	GloMoSim	NO	NO	NO	YES
	EAAR [70]	AODV,MMBCR, AntHocNet	GloMoSim	NO	NO	NO	YES
	AntHocMMP [71]	AntHocNet,LAR, R-ACO1,MMP	NS-2	YES	YES	YES	YES
	ACECR [72]	AOMDA, EAAR	NS-2	YES	YES	NO	YES
	Hybrid ACO [74]	Normal ACO	unknown	NO	YES	NO	YES
Location aware	POSANT [77]	AntNet, GPSR, AntHocNet	own simulator [77]	YES	YES	YES	NO
	Robustness-ACO [78]	AntHocNet, LAR	own simulator [78]	YES	YES	YES	YES
	MAR-DYMO [79]	AODV,DYMO, Ant-DYMO	NS-2, VNMG [83]	YES	YES	YES	NO
	MAZA-CORNET [82]	AODV,AMODV, GPSR	NS-2, VanetMobiSim [106]	YES	YES	YES	YES
	Cluster-based ACO [85]	AODV	NS-2,VNMG	YES	YES	YES	YES
	S-AMCQ [86]	IAQR [107],AMCQ [86]	OMNet++	YES	YES	NO	YES
Security aware	SAR-ECC [87]	without	NS-2	NO	NO	NO	YES
	SPA-ARA [89]	AODV,DSR,ARA	SWANS [108]	NO	NO	NO	YES
	FTAR [96]	ANT-U	NS-2	YES	YES	YES	YES
	SBDT [97]	CAPMAN	NS-2	YES	YES	NO	YES
	DBA-ACO [98]	without	NO	NO	NO	NO	NO
	ANTNET [99]	without	NS-2	NO	NO	NO	YES
	ABPKM [100]	without	QualNet	YES	YES	YES	YES

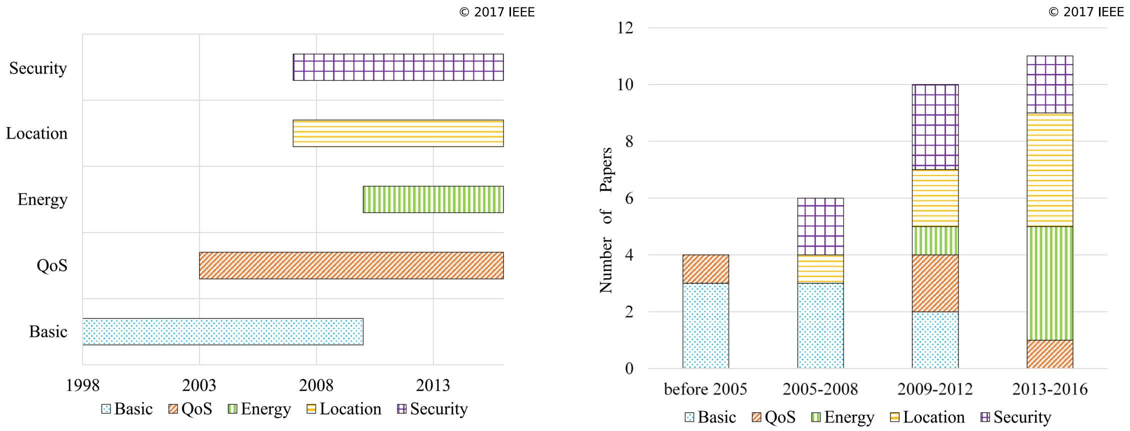
aware ACO routing protocols consider these three metrics as important performance metrics.

In contrast, the other three categories have more special performance metrics due to their design aims. Besides the previously mentioned metrics, data throughput, the scalability of the network and the hop counts of connections are the most popular metrics used by many protocols from all the five main categories. Moreover, there are some other particular special metrics for different categories due to their special pertinence. For example, in the energy aware ACO routing category, ACO-EEAODR [69] and EAAR [70] have not illustrated any common metrics. ACO-EEAODR only compared the energy consumed in path selection and the network lifetime. EAAR uses six performance metrics for the comparison of their protocols with others, which are the number of dead nodes, the number of packets dropped, the total energy consumed, the number of packets delivered, the energy per packet delivered, the packets delivered per dead node and the packets dropped per packets delivered. The network lifetime, the dead node ratio and the energy consumed are the most popular performance metrics for all surveyed protocols in this category.

In the security aware ACO routing category there are also many special metrics. Except for DBA-ACO [98], which has no implementation, all of the other protocols in this category are evaluated using special metrics. Moreover, 50 % of these protocols have only focused on evaluation using their own special performance metrics. For instance, in SBDT [97], the authors have shown the detection accuracy which represents how well the algorithm detects security threats. In SAR-ECC [87] the authors have presented the successful rate of packet forwarding, the authentication cost and the necessary packet rate vs. the speed of nodes. Another protocol SPA-ARA [89] also shows the energy consumption, the number of successfully found routes and the number of packets dropped by the malicious nodes. From observations, it indicates that security aware ACO routing protocols consider the security related metrics more important than the general benchmarking metrics, such as end to end delay. In other words, in order to guarantee security during network communication, these protocols made a trade-off between the security level and performance. However, due to the different scope aimed at by these protocols targeting various security issues, there are not many common special performance metrics. This could be a reason to answer the question why 50 % of protocols in this category have not made any comparison with related work.

Another observation shows that although many of the surveyed protocols have shown good performance in small networks, the scalability of the proposed protocols has not been demonstrated. In contrast, in [96] the authors have shown the DDR, delay and overhead metrics over increasing the network sizes and mobility rates respectively. Besides the common performance metrics related to the scalability, in [100] the authors have also shown the successful rate of finding certificate chain, the reliability of selected honest certificate chains and other special metrics which describe the performance of the proposed approach.

From the reviewed ACO-based routing protocols in this paper, it can be clearly seen that significant efforts have been made to address the requirements of efficient and effective routing protocols for



(a) The development.

(b) The proportion.

Figure 2.4: ACO-based routing protocols in MANETs.

MANETs. The results of the comparison based on protocol design and simulation parameters are presented in section 2.2.4 and 2.2.5. Certain drawbacks in the considered routing protocols are also identified. First of all, most of the reviewed approaches in all five categories have not been evaluated with large networks. Although all the surveyed protocols have shown good performance in small networks, the scalability of the proposed protocols has not been demonstrated. Secondly, most of the location aware protocols have not mentioned security or authentication and all the proposed protocols in VANETs completely lack practical testing via real-time traffic models. Finally, in the security based ACO routing category, more than 50 % of the protocols only do self analysis and no comparison with other standard routing protocols are done.

Discussion

In this section the development history of the five main categories is summarized and future possible design directions of ACO-based routing protocols are also discussed.

Figure 2.4a shows the development history of all surveyed papers of the five main categories in the past 19 years. Designing effective and efficient protocols to address only the basic requirements of routing in MANETs used to be a hot topic. Due to the dynamic nature of ACO's connectivity, ACO is able to continuously find the optimal routes in real time despite the topology changes in the network. Therefore, researchers began to apply ACO algorithm to solve the routing problem in MANETs. The first ACO-based routing protocol was proposed in 1998. Since then many subsequent researchers have focused on this direction for more than ten years. In the early blossoming stage of ACO-based routing algorithms, QoS in routing was an important aspect in MANETs and until now QoS aware ACO-based routing protocols have been studied for over than 13 years. The other three categories shown in figure 2.4a are relatively new directions which have been developed within the last ten years.

Figure 2.4b illustrates the number of proposed ACO routing papers during different periods in time. Before 2005 there were only few proposed protocols, therefore they are summarized in one time span. From 2005 on, the number of papers over four year periods is shown for each category. It can be seen that most of the publications are focused on basic ACO-based protocols in MANETs before 2008. After 2010 there is no further study in this category. Since 2007 the three new research directions of energy aware, location aware and security aware ACO-based routing protocols have attracted more and more researchers. Therefore, designing routing protocols which aim only for finding the optimal routes was no longer the focus of this research area. While in the period from 2005 to 2008 there was no new QoS aware ACO-based routing protocol, this field continues to be actively studied up to now. QoS will always need to be improved as it remains a priority to satisfy users' communication requirements. In recent years, energy efficiency is becoming an independent and significant issue in designing ACO-based routing protocols. In figure 2.4b the number of energy aware ACO-based protocols rises up significantly after 2009, from 10 % of all protocols in the third time slot to 36 % in the fourth time slot. However, some of the energy aware protocols make trade-offs with respect to path length or route delay. Further research in this area is still necessary to resolve these open issues.

During the last ten years, location information aware vehicle routing is becoming a hot topic, due to the increasing ubiquity of GPS. Location information aware routing protocols have been widely used, especially in VANETs. From the reviewed ACO-based routing protocols in VANETs, most of the protocols are designed for Vehicle-to-Vehicle (V2V) networks. As the V2I communication networks develop progressively, in the future new protocols will be proposed in this area. Moreover, since most of the reviewed protocols do not consider any security issues, designing security and location aware ACO-based routing protocols in MANETs, would be an interesting future research direction. S-AMCQ [86] is a good example. At the same time, security aware protocols themselves are also a growing field. The proportion of this category remains stable. New protocols in this category are needed to reduce overhead and delay introduced by the security mechanisms, such as authentication processes. Moreover, combining security and other metrics would be valuable. For example, security and energy aware ACO-based routing protocols that avoid repeated usage of the optimal secure path could be designed and studied. Combining security and location aware ACO routing protocols for usage in VANETs also seems promising. All in all, designing QoS, energy, location and security aware ACO-based routing protocol are four main research directions. There are still open questions in each direction which encourage researchers to study further. However, considering multiple issues in the design of a routing protocol can make the protocol more suitable for real world applications. Therefore, designing ACO routing protocols based on the multiple existing issues in MANETs and especially in VANETs, would be an interesting future research direction.

2.2.6 Summary

Due to the self-organizing properties of MANETs, routing is considered a challenging problem. The ACO meta-heuristic which presents a common framework for approximating solutions to NP-hard optimization problems is especially applicable to dynamic problems, such as routing in MANETs. In the past two decades, researchers have designed various ACO-based routing protocols in MANETs. Section 2.2.2 introduces mainly the ACO algorithm and the existing ACO-based routing protocols in MANETs from 1998 up to now. The reviewed protocols are sorted into five main categories and a detailed comparative analysis in terms of protocol design and simulation related parameters for all reviewed protocols is presented. Besides the reviews and comparisons, the open issues of the surveyed protocols are also discussed. Finally, based on the observations, the changes in research interests over the years are summarized and the promising future directions for research in ACO-based routing protocols are also discussed.

2.3 Security attacks in MANETs

Due to the wireless properties, nodes in MANETs are vulnerable to network attacks. This section will introduce the general classification of security attacks in MANETs and also presents some of the well-known attacks, specially the attacks that target the network layer.

2.3.1 Classification of attacks in MANETs

As introduced in section 2.1.1, MANETs have special properties which are different from the wired networks. However, these special properties lead to many general security vulnerabilities. First, MANETs are infrastructure-less networks and there is no central trusted authority, which can take care of the security threats for the whole network. Therefore, security solutions must adapt to the distributed architecture of MANETs. Secondly, nodes in MANETs are free to move in the whole network area and they can leave and join the network at any time. The high flexibility of nodes movement leads to the frequent topology changes in MANETs. Therefore, it is more difficult to recognize the selfish or malicious behaviors of nodes in the network. Thirdly, bandwidth in MANETs is restricted and due to the nature of the shared wireless transmission channel, adversaries can launch interference to make congestions or monitor the network traffic. Furthermore, ad hoc nodes usually have limited battery power and restricted data storage capacity and computational power. However, security solutions usually require more resources, due to cryptography operations or other security related operations. Therefore, achieving security in MANETs is more challenging as that in wired networks. Finally, the physical protection of mobile ad hoc nodes is usually not very strong. In hostile environments, mobile nodes are likely be damaged or compromised by attackers and used for launching an internal attack which is hard to be defended.

There exist many security attacks for MANETs and according to the attack means, these attacks can be generally categorized into two groups, namely passive attacks and active attacks [109].

Passive attacks

This type of attacks is launched by attackers who want to hide their presence from the network. Therefore, passive attacks do not interrupt any network functionalities, but they aim for collecting valuable information, such as the identity of the important nodes in the network or the location of nodes, through monitoring and analyzing the network traffic.

An example of passive attacks is the eavesdropping attack [110]. Since a packet sent by a node can be heard by all its neighbor nodes which are equipped a transceiver, if the packet is not encrypted at all, then attackers can easily get valuable information from the network traffic. Furthermore, the sender and receiver are hardly able to notice that their packets are eavesdropped. Defending against passive attacks is very difficult since there is no direct evidence to reveal the existence of such attacks. The recommended countermeasure is to apply powerful encryption techniques.

Active attacks

In active attacks adversaries launch intrusive operations such as modifying, fabricating, injecting, forging or dropping packets, thereby leading to disruptions of the network communication. The effect made by active attacks can be so severe that the network performance is degraded significantly. In the worst case, attackers can even bring down the entire network. There are many types of active attacks. Base on where the attacks take place regarding to the Open Systems Interconnection model (OSI model) [111] layer, attacks can be further divided into Medium Access Control layer (MAC layer) attacks, network layer attacks, transport layer attacks, application layer attacks and the others.

2.3.2 Security attacks in MANETs based on OSI model

Some of the well-known attacks in MANETs is presented in table 2.12 based on OSI model layers.

Table 2.12: Security attacks in MANETs based on OSI model

OSI model layer	**Security attacks**
MAC layer	jamming, GTS, etc.
Network layer	black hole, flooding, etc.
Transport layer	session hijacking, etc.
Application layer	repudiation, etc.
Others	DoS, etc.

MAC layer attacks

MAC layer attacks aim for disturbing the availability of the Mac layer, such as the jamming attacks [112]. Since the wireless channel is shared with every participants in the network, attackers are able to launch different kinds of interference to jam the frequency channels which leads to the deny of services for legal users in the network. A jammer can interfere with legitimate wireless communications either by preventing a node from sending out packets, or by preventing the reception of packets by the node. Another example in this type of attacks is the Guaranteed Time Slot (GTS) attack [113]. A malicious node in a GTS attack can extract the GTS descriptor within beacon frame and analyze the GTS times of the coordinator. Whenever it obtains the allocated GTS times, the malicious node is able to create interference which causes collision of the data packets between the normal node and the coordinator node.

Network layer attacks

Since the routing protocols can establish and facilitate the connections among wireless devices in MANETs, they are the foundation of MANET applications. However, due to the absence of infrastructure and the shared wireless communication channel, nodes in MANETs are very susceptible to attacks and the traditional security mechanisms applied in the wired networks are not suitable for MANETs. Various types of network layer attacks are exposed and studied by researchers. Some of well-known network layer attacks are introduced as below:

Black hole attacks [114]: As soon as receiving a route request packet, a black hole node advertises itself as having the shortest path to the destination node. As most protocols prefer to use the shortest path for data transmission, the black hole node are likely be chosen in the route. Therefore it can then drop data packets or perform message modification attacks.

Gray hole attacks [115]: Gray hole attacks can be considered as a variant of black hole attacks. In stead of dropping data packets constantly, the gray hole node can switch its states between normal and malicious behavior. In the route discovery phase, it may behave normally, but it may drop data packets in the data forwarding phase. As normal nodes might drop packets due to congestion, the detection of a gray hole node is not easy.

Wormhole attacks [116]: This type of attacks is launched by at least two colluding attackers. The attackers connect with each other through a long-range wireless link or even through a wired link. Once an attacker receives packets at one position in the network, it tunnels them to the other attacker which is located at another position in the network, and the other attacker then replays these packets into the network at that new position.

Flooding attacks [117]: Flooding attack in network layer is a type of resource consumption attacks which try to waste away resources of normal nodes in the network, such as battery power, bandwidth, and computational power. Flooding nodes in this attack usually broadcast fake routing packets, such as the route request packets. Other nodes in the network have to forward these routing packets and consume their recourses.

Transport layer attacks

Session hijacking attack [118] can be launched by using off-the-shelf hardware and software. It can combine with Denial of Service (DoS) and identity spoofing attacks. For example, in a session hijacking attack the adversary disrupts a ongoing session by forcing a legitimate mobile station to terminate its connection to an access point first. Then the adversary can masquerade itself with the MAC layer address of the disconnected mobile station and associate with the access point.

Application layer attacks

In a repudiation attack [119], the attacker accesses the network, but denies completely or partly of the participation in the network communications.

Other attacks

Besides these attacks which are launched in a single OSI model layer, there are also attacks which are usually launched through multiple OSI model layers, such as DoS attacks [120]. Attackers in DoS attacks aim to deny network services to legitimate nodes. According to the targeted type of service, DoS attacks can be launched in different OSI model layers. For example, if the attacker aims to deny the network service, then it can launch the flooding attacks by broadcasting fake route request packets which is targeted to a non-existing node in the network. These fake control packets are flooded in the network and the normal service in network layer is disturbed. Another example is the session hijacking attacks in the transport layer. Since the attacker in a session hijacking attack can control a ongoing session, it can cause the denial of service for the legitimate nodes in the session.

2.4 Attack Models

After introducing the overview of the existing network layer attacks in MANETs, the attack models [121], [122] implemented in the experiments are introduced in this section.

2.4.1 Black hole attack

Since packet-dropping attacks are a major threat to the security of MANETs [23], in this work the black hole attack introduced in [114] is chosen as one of the attack models to investigate SAFEACO's performance.

As shown in figure 2.5, node M is a black hole node. When the source node S attempts to find a route to destination node D, S sends out FANTs to discover the network. As soon as node M receives the FANT, it replies immediately with a BANT which contains a fake route. This fake

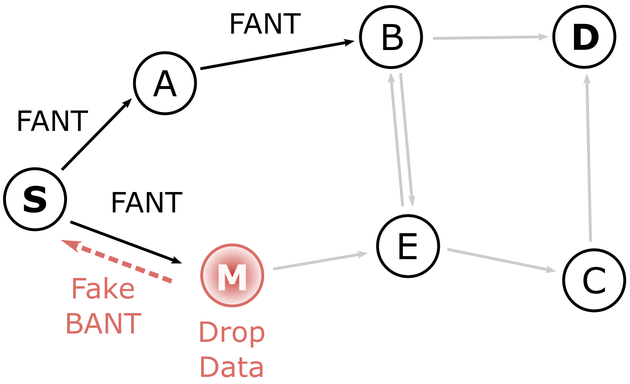


Figure 2.5: Black hole attack model.

route will designate itself as the shortest or optimal route. If the source node does not have any mechanism to detect malicious behavior, it will be deceived and will send all data packets to the black hole node, which simply drops them.

2.4.2 Sybil attack

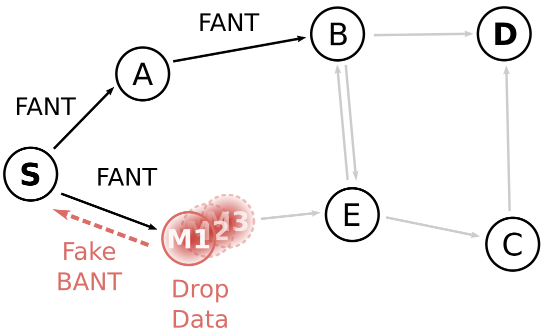


Figure 2.6: Sybil attack model.

In 2002 J. R. Douceur first introduced the Sybil attack [123] in context of peer-to-peer networks. In the Sybil attack, a malicious node presents multiple identities to the other nodes in the network. C. Karlof and D. Wagner pointed out that the Sybil attack can threaten the routing mechanism in wireless sensor networks [124]. J. Newsome et al. established a classification of different kinds of the Sybil attack in [125]. According to this classification, Sybil attacks can be divided into simultaneous and Non-Simultaneous attacks. In the first group, a Sybil node may try to present all its Sybil identities to the network in the same time. Since a particular hardware entity can only show one identity at a time, it can cycle through all its identities to let other nodes believe that all the identities are a group of nodes which exist simultaneously in the network [125]. In the other group, a Sybil node can let one or a group of its Sybil identities leave or join the network at any given time [125].

In this work, a special case of the non-simultaneous Sybil attack is implemented. A Sybil node has multiple (at least two) Sybil identities. Every Sybil identity is not duplicated with any other nodes' identity in the network. Sybil node presents only one of its identities to the network at a time, but it switches its identity in a predefined interval, for example, in every 50 seconds. However, if the Sybil node only switches its identities in the routing process, it does not affect much the routing performance. In order to better understand the effects made by the Sybil attack, the black hole attack is embedded into the Sybil attack in the way that each Sybil identity can launch the black hole attack. Figure 2.6 shows that a Sybil node M with two extra hidden identities in the network. In the experiments, node M has three identities: $M1$, $M2$ and $M3$. In every 50 seconds, node M switches its identities and it uses the current identity to launch the black hole attack until the next switch moment.

2.4.3 Flooding attack

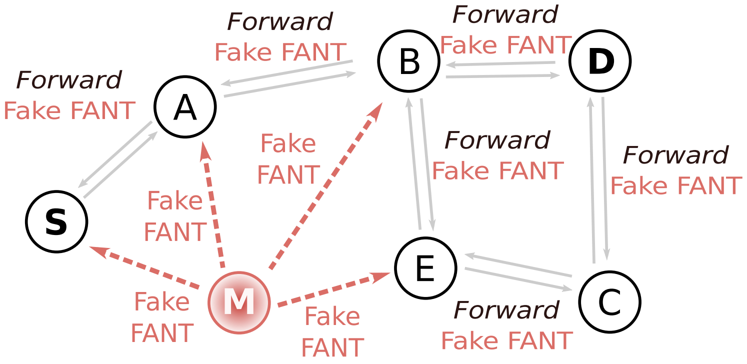


Figure 2.7: Flooding attack model.

The main target of the flooding attack [117] is to consume network resources, such as bandwidth, to exhaust the energy available to nodes energy or their computational power, to disrupt the routing process in the network. This kind of attack doesn't aim at the resources of some particular nodes, but the resources of the whole network. In this attack mode, a flooding node broadcasts excessive RREQ packets with non-existing destination Internet Protocol (IP) addresses. In this case, no one in the network could reply the these RREQs and as consequence the network will be full of such fake RREQs.

In this work, instead of RREQ packets the flooding nodes regularly broadcast fake FANTs which include a non-existing IP address as the destination node. Since normal nodes can not directly notice that the destination IP address doesn't exist in the network, they will forward the fake FANT to their neighbor nodes. In order to make the flooding nodes more difficult to be detected, the attack node is set to flood the fake FANTs every three seconds in the implementation.

Chapter 3

SAFEACO in MANETs

Inspired by other ACO routing algorithms, a security aware fuzzy enhanced ant colony optimization routing protocol in MANETs is proposed. The aim is to design a routing protocol in MANETs which can provide a high packet delivery ratio, low end-to-end delay and low communication overhead in normal scenarios as well as in attack scenarios. Therefore, SAFEACO has to guarantee both efficiency and security as a routing protocol for MANETs. The primal ideas of SAFEACO routing protocol have been introduced mainly in [121, 122, 126].

Since AntHocNet [127], with its hybrid architecture, shows convincing performance and it has been proven to be more efficient than other state-of-the-art routing protocols in MANETs, such as AODV, its routing structure is applied in SAFEACO. Therefore, there are four similar processes in SAFEACO as those designed in AntHocNet, namely the reactive route discovery, the proactive route maintenance, the data transmission and the handling of link failures.

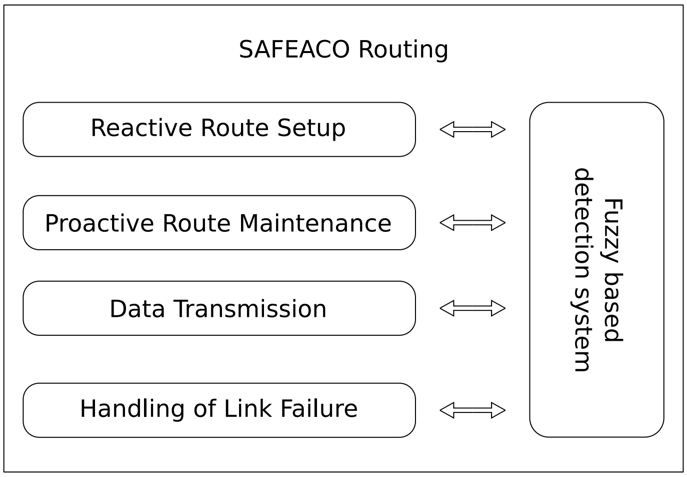
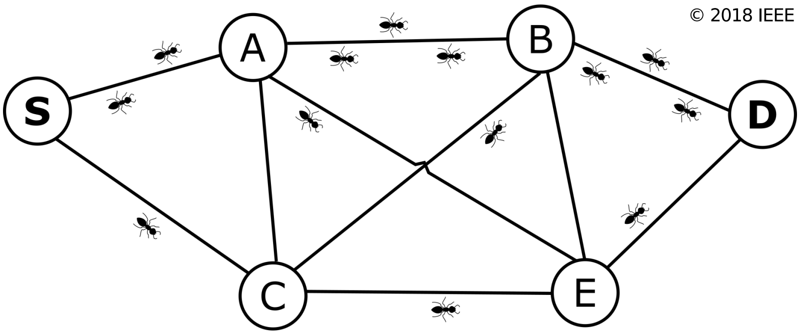


Figure 3.1: General routing structure of SAFEACO.

Section 3.1 presents the reactive route discovery in SAFEACO, while section 3.2 introduces the proactive route maintenance in SAFEACO. The data transmission process is introduced in section 3.3 and section 3.4 presents the handling of link failures in SAFEACO. Figure 3.1 gives an overview of the general routing structure of SAFEACO.

3.1 Reactive Route Setup in SAFEACO



© 2018 IEEE

Figure 3.2: SAFEACO in a MANET.

In order to apply the ACO algorithm to the problem of routing in MANETs, the network has to be represented as a graph [49]. Figure 3.2 shows an example, where an optimal route between the nodes S and D should be found. Ants can only travel along the edges of the graph, which represent the communication links between the nodes participating in the network.

Figure 3.3 introduces the flowchart of the reactive route setup process. To find a route, node S broadcasts reactive FANTs. The probability for a reactive FANT which starts from node i to choose node j as the next hop is defined as in equation 3.1 [121,122,126].

$$P_{ij}^{d}(t) = \frac{\left[\tau_{ij}^{d}(t) \cdot R_{ij}(t)\right]^{\alpha}}{\sum_{l \in N_i^d}\left[\tau_{il(t)}^{d} \cdot R_{il}(t)\right]^{\alpha}} \quad , \forall j \in N_i^d \tag{3.1}$$

In this equation, $P_{ij}^{d}(t)$ is the probability of an ant moving from node i to node j on the way to the destination node d at the t-th iteration step or time slot; N_i^d is the set of current neighboring nodes of node i, over which a route to node d is known; $\tau_{ij}^{d}(t)$ is the regular pheromone intensity on the link between nodes i and j on the way to destination node d at t-th iteration step or time slot; $R_{ij}(t)$ is the reliability value estimated by the fuzzy detection system in section 3.5 for the link between nodes i and j at the t-th iteration step or time slot; $\alpha \geqslant 1$, is a parameter which controls the exploratory behavior of the ants. α is set to 20 in the experiments, which is the same value used in AntHocNet [127].

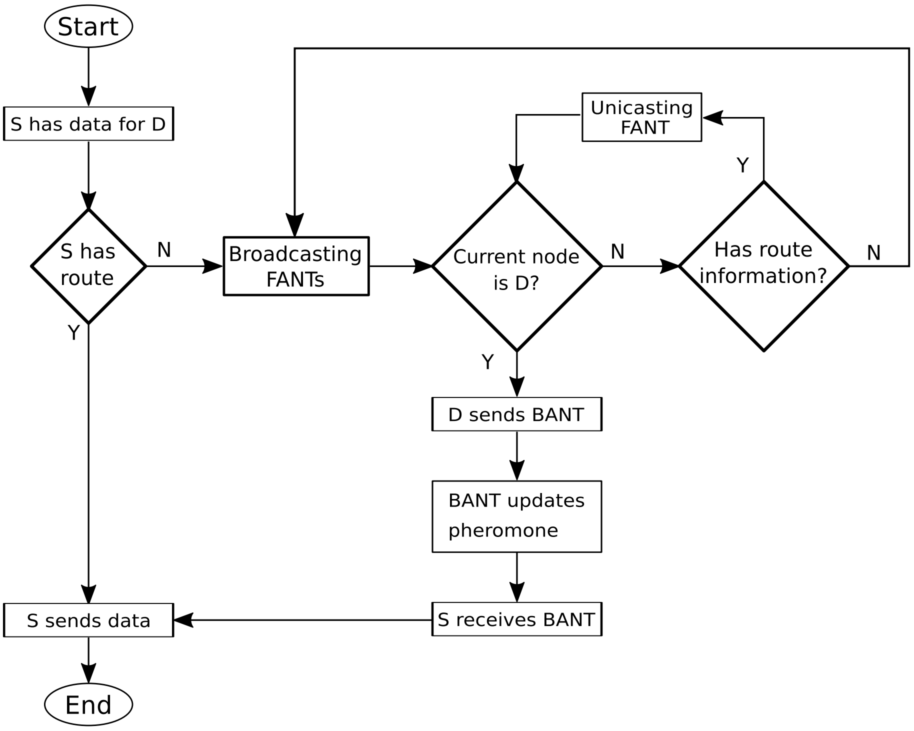


Figure 3.3: The flowchart of the reactive route setup process.

As shown in figure 3.3, the reactive FANT is either unicast or broadcast at each intermediate node, depending on whether the current node has routing information for the destination. In order to limit the overhead caused by broadcasting ants, intermediate nodes only forward the first copy of any received ants. A reactive FANT moves hop by hop until it reaches the destination node or until the maximum travel hop count of the ant is reached. For each step, it chooses one of its neighbor nodes according to equation 3.1.

After the ant arrives at the destination node, it turns into a BANT and travels back to the source node by following exactly the same route. At each intermediate node, the BANT updates the cost value C_{id} by adding the last hop's cost value C_{in} to it. C_{id} represents the cost of sending a packet from node i to node d along this route. The amount of pheromone updates assigned to a link is calculated based on the quality of the route in which this link is involved, and the pheromone evaporation rate, as shown in equation 3.2 [127]. An ant considers the quality of a route to be an amount that is inversely proportional to the cost of the route C_{id}. The pheromone evaporation rate is predefined and allows ants to forget outdated routes and to explore new routes.

$$\tau_{ij}^{\text{new}} = \rho \cdot \tau_{ij}^{\text{old}} + (1 - \rho) \cdot \frac{1}{C_{id}} \tag{3.2}$$

τ_{ij}^{old} is the previous regular pheromone value on the link between nodes i and j; τ_{ij}^{new} is the updated regular pheromone value on the link between nodes i and j; $\rho \in (0, 1]$ is the pheromone evaporation rate. In the experiments, ρ is set to 0.7, which is same as in AntHocNet [127].

Since C_{id} is the total cost of sending a packet from node i to node d along this route, let node a and node b be the arbitrary adjacent two nodes in this route and let C_{ab} represent the cost of sending a packet toward node d from node a to node b. C_{ab} is calculated based on Signal-to-Noise Ratio (SNR) as shown in equation 3.3 [127].

$$C_{ab} = \begin{cases} 1 & \text{if} \quad \text{SNR} > \text{SNR}_t \\ C_{\text{const}} & \text{if} \quad \text{SNR} \leqslant \text{SNR}_t \end{cases} \tag{3.3}$$

SNR_t is the predefined threshold value of for the SNR, at which a link is considered to be bad; C_{const} is the cost of using a bad link. In the experiments, SNR_t is set to $17\,\text{dB}$ and C_{const} is set to 3, which are the same values used in the original AntHocNet implementation [127].

After the route to the destination is discovered successfully, data packets are ready for transmission. This process is introduced in section 3.3.

3.2 Proactive Route Maintenance in SAFEACO

In order to improve routing efficiency, a proactive route maintenance mechanism which consists of pheromone diffusion and proactive ant sampling is also proposed in SAFEACO.

3.2.1 Pheromone Diffusion

In this process, node i, chooses randomly up to 10 destinations to which it has valid routing information. It creates a list of these destinations, their corresponding best pheromone values and a flag that shows whether the best pheromone is a regular pheromone value or a virtual (or bootstrapped) pheromone value for the route. Node i adds this list to its *hello message* and broadcasts it regularly to all neighbor nodes. After receiving a *hello message* from node i, the neighbor node j, checks the routing information in the *hello message*. For each reported destination node in the list, node j estimates separately a bootstrapped pheromone value from itself to this destination node d. The exact formula is given in equation 3.4 [127].

$$K_{ji}^{d} = ((V_i^d)^{-1} + C_j^i)^{-1} \tag{3.4}$$

In the equation, K_{ji}^{d} denotes the bootstrapped pheromone value of node j to destination d via neighbor node i; V_i^d is the reported pheromone value of this route, which indicates the quality of the best route from node i to node d; C_j^i is the locally maintained cost value of hopping from node j to node i.

In order to keep the pheromone obtained from the pheromone diffusion process separate from the regular pheromone, which is obtained in the reactive route setup process, it is stored as a virtual pheromone value, denoted as ω_{ji}^{d}. This denotes the virtual pheromone of node j to destination d via neighbor node i. ω_{ji}^{d} is assigned the value of K_{ji}^{d}.

The additional overhead caused by this step is negligible, because adding the table to the *hello message* only increases its size by a few bytes. No additional control packets need to be sent out, so no additional media access control overhead is introduced either.

3.2.2 Proactive Ant Sampling

In the proactive ant sampling process, source nodes send out proactive forward ants regularly to gather routing information for ongoing data sessions. In the experiments, during data sessions, proactive forward ants are sent out every second. Proactive forward ants apply a probability rule described in equation 3.5 [121,122] to choose their next hop.

$$P_{ij}^{d}(t) = \frac{(\max\left[\tau_{ij}^{d}(t), \omega_{ij}^{d}(t)\right] \cdot R_{ij}(t))^{\alpha}}{\sum_{l \in N_i^d}(\max\left[\tau_{il(t)}^{d}, \omega_{il}^{d}(t)\right] \cdot R_{ij}(t))^{\alpha}} \quad , \forall j \in N_i^d \tag{3.5}$$

This rule is similar to the one described in equation 3.1. In the experiments, the α used in equation 3.5 is set to 2. Once the proactive ant reaches its destination node, it is converted into a proactive backward ant which has the same behavior of a reactive backward ants. It updates the regular pheromone values on its way back to its source node.

As consequence, the attractive virtual pheromone values obtained from the pheromone diffusion process can be investigated by the proactive ants in the proactive ant sampling process and, if the proactive backward ant comes back, a new route is found for data transmission.

3.3 Data Transmission in SAFEACO

After the setup of the route, data packets are forwarded hop by hop towards their destination node. Different from DSR protocol in which the route information is included in the packet header, the routing information is distributively stored in the pheromone tables at each intermediate node.

Therefore, each hop makes the routing decision for forwarding data packets to the next hop. One thing worth to be noticed is that only the regular pheromone is considered in the routing decisions.

In SAFEACO, nodes forward data packets stochastically, based on the different regular pheromone values saved in the pheromone table for the targeting destination node. The probabilistic decision rules used to chose the next hop for data packets is described in equation 3.6.

$$P_{ij}^{d}(t) = \frac{\left[\tau_{ij}^{d}(t) \cdot R_{ij}(t)\right]^{\beta}}{\sum_{l \in N_i^d} \left[\tau_{il(t)}^{d} \cdot R_{il}(t)\right]^{\beta}} \quad , \forall j \in N_i^d \tag{3.6}$$

$P_{ij}^{d}(t)$ is the probability of an data packet moving from node i to node j on the way to the destination node d at the t-th iteration step or time slot; N_i^d is the set of current neighboring nodes of node i, over which a route to node d is known; $\tau_{ij}^{d}(t)$ is the regular pheromone intensity on the link between nodes i and j on the way to destination node d at t-th iteration step or time slot; $R_{ij}(t)$ is the reliability value estimated by the fuzzy detection system in section 3.5 for the link between nodes i and j at the t-th iteration step or time slot; $\beta \geqslant 1$, is a parameter which can control the exploratory behavior of the ants.

This rule is the same as the one used by the reactive forward ants as shown in equation 3.1 in section 3.1, except the parameter β. In order to adapt the relative preference for the best routes for data and ants separately, β can be set to a different value as the one used for α in equation 3.1. Generally speaking, by setting β value low, data packets are forwarded over multiple routes which can improve the network throughput, but in this case, routes with low pheromone values are also considered in the data transmission. On the other hand, data packets are concentrated on the best routes when β value is high. In the experiments, β is set to a relative high value 20, which is used in AntHocNet [127], as only good routes of more or less equal reliability should be used for the data transmission.

3.4 Handling of Link Failures in SAFEACO

Due to the movement of one node or the change of radio interference or transmission power, link failure may occur frequently in MANETs. In SAFEACO, link failure detection is either caused by the failed unicast transmission of control packet or data packets from lower layer or via the used of *hello messages*. The first detection is based on the MAC layer protocol which usually has a mechanism to inform the upper layer about the success or failure of a unicast transmission. The second detection is based on the *hello messages* sent periodically by all the nodes in the network. If one node does not hear from a certain neighbor node for a given time interval which is set to two *hello message* intervals in the experiments, then this node assumes that the certain neighbor node disappears.

After detecting the link failure, SAFEACO reacts differently depending on how the link failure was detected. In case the detection was caused by the failed unicast transmission of control packets or the missed reception of *hell messages* in predefined interval, the node which detected this link failure first updates the entires which affected by this link failure in its pheromone table and then it broadcasts a link failure notification message. This message notifies the other surrounding nodes about this route change. After receiving a link failure notification message, nodes update their pheromone tables according to the information contained in the message. In case that the reported link failure affects their own routes, these node will further broadcast the link failure message.

If the detection is due to the failed unicast of a data packet, and the node which detected this link failure does not have an alternative route for this data packet, it will start a local route repair process to salvage the data packet. Assume node i detected a link failure and it does not have any alternative route, it buffers the data packet and sends out the repair forward ants which are identical to the reactive forward ants except that the repair forward ant can be broadcast a limited number of times. In the experiments, this number is set to 2. Therefore, the local repair process is similar to the reactive route setup process. Once the repair backward ant arrives the node i, node i can forward the buffered data packet to the destination node. If no backward ants come back to node i before the timeout occurs, then node i discards the buffered data packet and broadcasts a link failure notification message. In case that node i has already broadcasted the link failure message, but still receives new data packets from its upstream hop, node i will send out an unicast warning message to this node.

3.5 Malicious Behavior Detection in SAFEACO

Besides the basic routing mechanism, the malicious behavior detection system is presented in this section. The detection systems used in the MANET and VANET simulations are introduced respectively in section 3.5.2 and 3.5.3.

3.5.1 Why Use Fuzzy Logic?

In order to protect the network from malicious attacks, a distributed fuzzy logic based misbehavior detection system is proposed. Due to their inherent mobility in MANETs, usually only very limited information about the surrounding environment is available. Reasoning with only information about, e.g., neighboring nodes can be difficult for traditional approaches and provides insufficient amounts of data to perform online machine learning on nodes [121, 122]. These circumstances make fuzzy logic an appropriate choice, as fuzzy inference systems can operate with fuzzy data as it is usually available in this type of scenario. Benign nodes may drop packets due to channel congestion, interference or collisions, so assigning them a binary "reliable" flag would not be appropriate, while the softer categorization provided by a fuzzy logic system allows representing these nuances well.

3.5.2 Fuzzy Logic Based Detection System in MANETs

The first series of experiments in this work were launched in MANETs scope. For these experiments, the aim is to protect the network from black hole attacks and the Sybil attacks. More information about these two attacks are given in section 2.4. The detection system presented is shown in figure 3.4. The forward rate and the recent transmission were given to the detection system as input values, while the reliability is the output value of the detection system [121, 126].

Input Values

When a node sends a packet to be forwarded by another node, the sending node will keep listening on the radio channel to check if the receiving node actually forwards the packet within one second. Only the most recent 30 packets are watched for in this way by sniffing the link. The ratio of packets forwarded by a node to packets sent to a node corresponds to its *forward rate*. In the fuzzy system, this rate can either be "low", "medium" or "high". The membership function for this input value is given in Figure 3.5a.

The second input for the fuzzy system is the *recent transmission*, which is defined as the number of packets sent to a given node for forwarding, no matter if it was actually heard to be forwarded or not. Only packets from the last 30 seconds are considered here. The limitation of a maximum of thirty packets in total being considered, as described with regard to the *forward rate*, also applies.

© 2018 IEEE

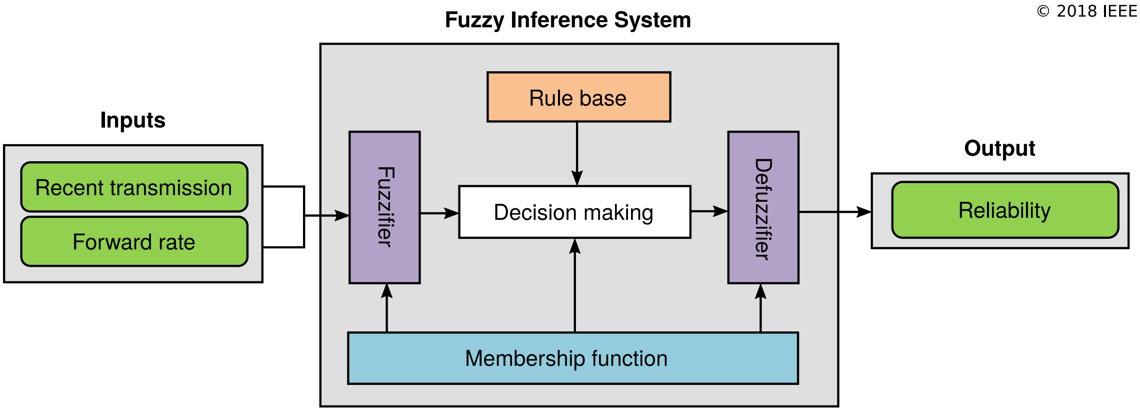


Figure 3.4: SAFEACO's fuzzy module in MANET experiments.

In the fuzzy system, this rate can either be "low", "medium" or "high". The membership function is given in Figure 3.5b.

Output Value

The fuzzy logic module performs fuzzy inference on the two input values and generates an output value called *reliability*. This output value can be either "very unreliable", "unreliable", "neutral", "reliable" or "very reliable". The membership function is given in figure 3.5c. This output value is then employed to make decisions regarding the routing process.

Fuzzy Rules

As shown in figure 3.4, the input values are first fuzzified by the fuzzifier in the fuzzy inference system, then, based on a number of predefined fuzzy rules and the membership functions the inferencing is performed. The result is defuzzified, which results in the final *reliability* value used in SAFEACO.

The rule base used for inference can be described as follows:

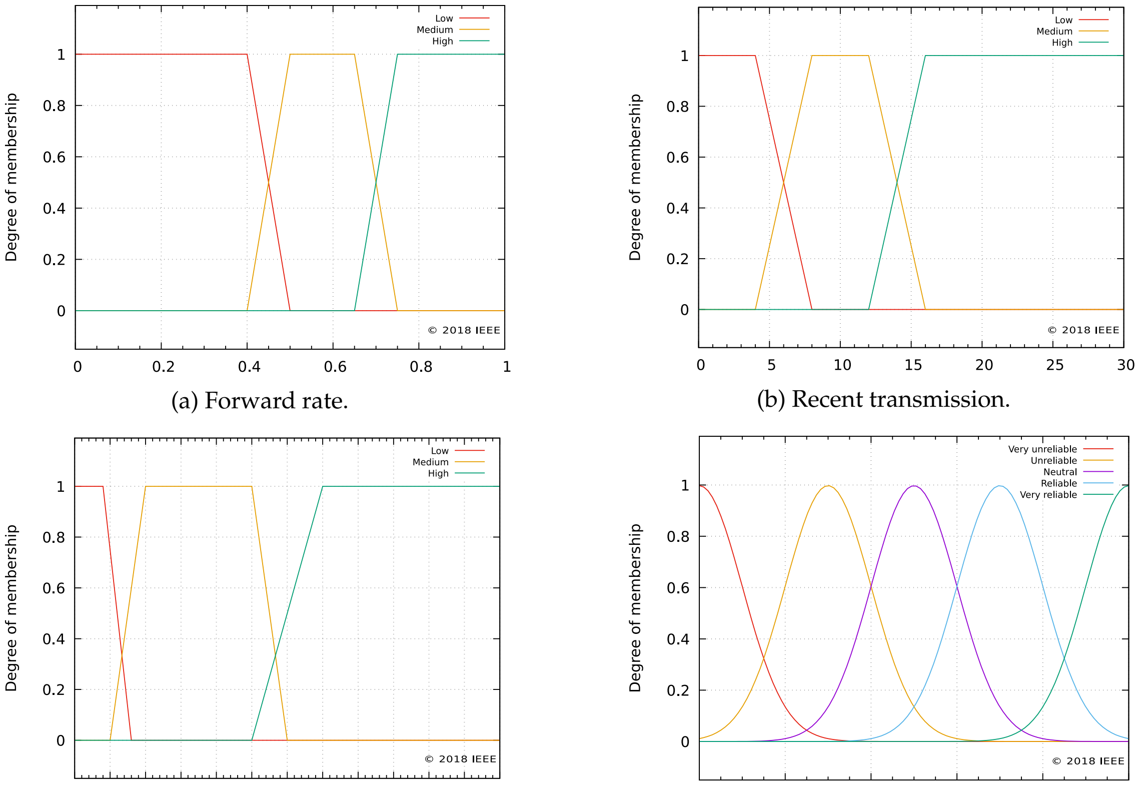
If the forward rate is *low* and the recent transmission is *low*, the reliability is assumed to be *neutral*, as not much is known about the behavior of the node. If the recent transmission is *medium* or *high*, the node is categorized as *very unreliable*.

If the forward rate is *medium*, the recent transmission values of *low*, *medium* and *high* each correspond to reliability values of *reliable*, *neutral* and *unreliable*.

Finally, if the forward rate is *high* and the recent transmission is *low*, the node is assumed to be *reliable*. For recent transmission values of *medium* and *high* it is assumed to be *very reliable*.

3.5.3 Fuzzy Logic Based Detection System in VANETs

The second series of experiments launched in VANETs is the extension of the first experiments launched in MANETs. These experiments aimed for investigating the performance of SAFEACO in VANET scenarios and also aimed for evaluating the robustness of SAFEACO under multiple attacks, for example, under the black hole and the flooding attacks in the same time. Therefore, some modifications are made to the detection system to detect the flooding attacks [122]. The following part presents more details.



(a) Forward rate.

(b) Recent transmission.

(c) Incoming rate.

(d) Reliability.

Figure 3.5: Membership functions for inputs (3.5a, 3.5b), 3.5c) and output (3.5d).

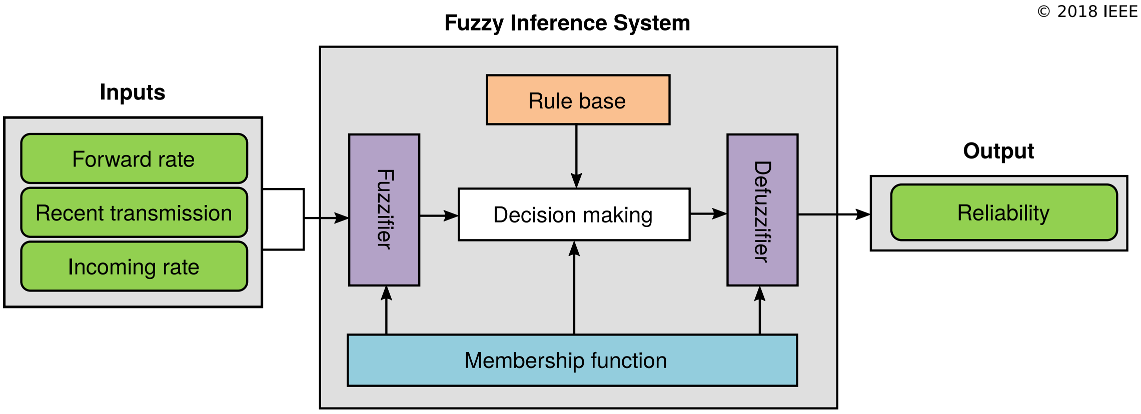


Figure 3.6: SAFEACO's fuzzy module in VANET experiments.

Input Values

Beside the two input values introduced in section 3.5.2, a third input value is added to the fuzzy detection system in VANET experiments. As shown in figure 3.6, it is the *incoming rate*, which is the number of received packets from one single neighbor node within a predefined interval. This parameter is an indicator that allows us to detect flooding nodes. In the fuzzy system, this rate can either be "low", "medium" or "high". The membership function is given in figure 3.5c. The output value of the fuzzy detection system in VANETs is also named "reliability". Its membership function is the same as introduced in figure 3.5d.

Fuzzy Rules

As shown in figure 3.6, the fuzzy inference system used in VANET experiments is similar to that used in MANETs experiments except the different fuzzy rule bases. Due to the modification of the input values, the corresponding fuzzy rules based are changed to the new rules which are described in table 3.1. In this table, a vector (a, b, c) means, that the *forward rate* is has value a, the *recent transmission* has value b and the *incoming rate* has value c, which possible values being **L**ow, **M**edium and **H**igh.

3.5.4 Fuzzy Inference System

SAFEACO enhances AntHocNet with a distributed fuzzy logic based malicious behavior detection system based on a traffic monitoring system. Since the traffic monitoring system only observers traffic in the network, the detection system does not cause any additional control packets in the routing protocol. In MANET experiments, every node monitors each of its neighbor nodes' behaviors and passes the observed parameters, namely the forward rate and the number of recent transmissions of packets to be forwarded, into its fuzzy inference system. In VANET experiments, an additional parameter, incoming rate, is also given to the fuzzy inference system. The fuzzy inference system estimates the reliability value of the observed neighbor node. This reliability value represents the quality of the link to this neighbor node and it is used during the route

Reliability	**Input combinations**
Very reliable	(H, M, L), (H, H, L), (H, M, M), (H, H, M)
Reliable	(M, L, L), (H, L, L), (M, L, M), (H, L, M)
Neutral	(L, L, L), (M, M, L), (L, L, M), (M, M, M)
Unreliable	(M, H, L), (M, H, M)
Very unreliable	In all other cases

© 2018 IEEE

Table 3.1: Applied fuzzy rules

decision process for both reactive and proactive forward ants, as shown in equation 3.1 and 3.5. In the experiments, the threshold value of the reliability is set to 0.12. All nodes node whose reliability value is below the threshold are considered unreliable and will not be chosen by reactive or proactive forward ants. In the case that a node only has pheromone values for unreliable nodes, it will send out new reactive forward ants to discover new routes, which may result in additional overhead.

In MANET experiments, the forward rate and the number of recent transmissions of packets to be forwarded are chosen to detect black hole attacks and in VANET experiments, an additional input parameter is added to the fuzzy detection system and the corresponding fuzzy rules are also modified to detect the flooding attacks. If there is a need to consider other types of network layer attacks in the routing protocol, slight modifications of the input parameters and the fuzzy rules can fulfill the requirements. This shows the general flexibility of the fuzzy detection system, which allows it to be adapted to handle any concrete demands of an application.

Chapter 4

Implementation

In this chapter, the network simulators used in this work and the implementation parameters of both MANET and VANET scenarios are introduced in detail.

4.1 Network Simulator

In order to investigate the performance of SAFEACO when undergoing flooding, black hole and Sybil attacks, a network simulator is needed. There exist many network simulators. Basically they can be categorized into two gropes. The first group is the open source simulators, such as NS-2 [84], NS-3 [105] and OmNet++ [104]. The other group is the proprietary network simulators, such as QualNet [55]. Generally speaking, all the mentioned simulators are representative in their own group and could be applied for the general network simulations. The open source simulators are free for research and educational use and the proprietary ones are not free, but they usually could provide an easy to use GUI and visualization tools for data analysis. The scenario requirements are first considered. As introduced before, this research consists of two series of experiments. One is in launched in MANET scenarios and the other in VANET scenarios. In the second series, the set up of the street map, cars' mobility model, and other car related parameters are very important. Considering the requirements of the VANET scenarios, it can be seen that the QualNet simulator provides little support for this, while on the contrary the open source simulators work well together with the Simulation of Urban Mobility (SUMO) [128] tool, which is commonly used for setting up the VANET scenarios. Therefore, only the open source simulators which fulfill all the requirements will be further considered. Among the three open source network simulators, since NS-3 is the successor of NS-2, the final choice is then between NS-3 and OmNet++. Both of these two simulators are popular discrete event network simulators nowadays and could work together with the SUMO tool for VANET scenarios. After implementing small projects in them, the running time in OmNet++ is found to be a bit longer, thus the proposed protocol is finally implemented in the NS-3 simulator and its performance according to various metrics is compared to that of Enhanced Adaptive ACKnowledgment modified version (EAACKm), which is based on EAACK [23], but was modified slightly to ease implementation without negatively impacting performance under the given scenario.

4.2 Implementation in MANETs

In this section, the parameter settings which are used in the base scenario for MANET scenarios are introduced [121, 126]. The implementation of EAACK is also presented in detail.

4.2.1 Basic Scenario

In the basic scenario, there are 50 nodes in a rectangular area with dimensions of 500 m × 1500 m. It's assumed that the area is completely free of obstacles which could affect the nodes' movement or radio transmissions. Node mobility is modeled according to a modified RWP with a minimum speed to mitigate the known issues [73] with this model. The nodes move with a randomly selected speed between 5 m/s and 20 m/s and the pause time is set to 30 s. Radio transmission is modeled according to the Friis propagation model [129], with a transmission range of approximately 250 m. There are 10 Constant Bit Rate (CBR) sessions in the network. Each CBR session starts randomly between 0 s and 30 s. Each source node of a CBR session sends out 4 data packets per second, with a size of 64 B each. The total duration of each simulation run is set to 900 s. Table 4.1 summarizes some of the important parameters in the basic scenario.

Table 4.1: Parameter settings in MANET basic scenario

Parameters	**Value**
Number of nodes	50
CBR sessions	10
Maximum speed	20 m/h
Data send rate	256 bytes/s
Size of network area	500 m x 1500 m
Simulation duration	900 s

4.2.2 Implementation of EAACK

To ensure a fair comparison and ease the implementation in NS-3 [105], some modifications are made to EAACK. The modified version of EAACK is marked as EAACKm. The main difference is the use of a blacklist which replaces the use of the MRA messages originally used in EAACK. The blacklist is used to record nodes which do not send acknowledgments and isolate them in future sessions.

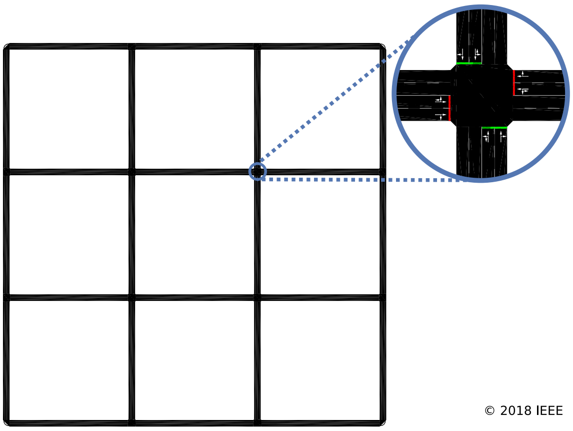
EAACK specifies an S-ACK mode. In this mode, for each consecutive sequence of three nodes in a route, the third node must send an acknowledgment to the first node. If the first node does not receive this acknowledgment, it reports both the second and third node as malicious. In this mode, a malicious node can easily make false reports against innocent nodes. The source node cannot verify these reports, unless it can find another independent route to the destination node and uses this to verify whether the destination node has received the reportedly missing data packet. In a highly dynamic network, it is not always guaranteed that multiple independent routes exist. Even if such routes exist, the delay incurred by such a verification process would be high. In order to avoid this problem, the implementation of EAACK is slightly different from the original design. When the first node receives the acknowledgment from the third node, it forwards this acknowledgment to the source node if it is not itself the source node. The source node records all received acknowledgments in a list. After a predefined interval, it checks the IDs inside the acknowledgments in the list and compares them to the route. This way, the source node is able to determine which nodes did not send an acknowledgment and can blacklist them. Nodes on the blacklist will not be chosen to be part of any future routes.

The proposed blacklist mechanism avoids sending extra control packets to finish the misbehavior report authentication process. Furthermore, it reduces the the delay caused by the authentication process and enables it to detect malicious nodes even in case that there does not exist an alternative route between the source and destination nodes. In other words, this modification could improve the detection rate and reduce both overhead and delay. Therefore, this modification in the implementation does not negatively influence the performance of EAACK and it does not reduce the security level of EAACK, since no fake misbehavior report attacks exist in the experiments.

Another difference is that the cryptography used in EAACK is not implemented to ease the implementation. The black hole attack implemented in the experiments only aims to drop data packets, not modify or record them. To ensure that packet sizes remain the same, padding is added to packets instead of signatures. Therefore, this difference does not influence the overhead and security level of EAACK.

4.3 Implementation in VANETs

In this section, the parameter settings which are used in the base scenario for VANET scenarios is introduced [122].



© 2018 IEEE

Figure 4.1: Traffic map generated in SUMO.

4.3.1 Basic Scenario

The SUMO [128] traffic simulator is applied for simulating the vehicular network scenarios. In the basic scenario, there are 70 vehicles in a square area with dimensions of 750 m × 750 m. The map is shown in figure 4.1. Each street is bi-directorial and each direction has two lanes. There are 16 traffic conjunctions altogether and the distance between adjacent traffic conjunctions is 250 m. The speed limit in each street is 50 m/s. The traffic lights are setup with SUMO default values. Radio transmission is modeled according to the Friis propagation model [129], with a transmission power of 20 dBm which approximately covers one ninth of the map's area. There are 10 CBR sessions in the network. Each CBR session starts randomly between 0 s and 30 s. Each source node of a CBR session sends out 4 data packets per second, with a size of 64 B each. The total duration of each simulation run is set to 1000 s. Table 4.2 summarizes some of the important parameters in the basic scenario.

Table 4.2: Parameter settings in VANET basic scenario

Parameters	**Value**
Number of vehicles	70
CBR sessions	10
Maximum speed	50 m/h
Data send rate	256 bytes/s
Size of network area	750 m x 750 m
Simulation duration	1000 s

Chapter 5

Evaluation

In this chapter, the evaluation of SAFEACO's performance over two series of experiments are introduced. The simulation results are also compared with other well-known routing protocols. The intermediate results have been introduced in [121,122,126].

5.1 Evaluation Measures

Five different measures have been chosen for the evaluation of the proposed approach:

5.1.1 Packet Delivery Ratio (PDR)

This parameter is calculated by using the total number of packets received by the destination nodes divided by the total number of packets sent by the source nodes [121,122]. The PDR's value is in the range of $[0, 1]$. Since the purpose of a black hole attack is to disturb the communication in the network by dropping packets, ensuring a high PDR value is the main goal of the approach. The formula is given as follows:

$$\text{PDR} = \frac{\text{\# packets received at destination nodes}}{\text{\# packets sent by source nodes}}$$

5.1.2 Overhead in Packets

The average overhead in packets is the total number of transmitted control packets divided by the number of data packets delivered.It should be noted that sending a forward ant from the source node to the destination node over n intermediate nodes, is counted as $n + 1$ transmissions, but sending a data packet instead, is counted as one packet being delivery. The overheads caused by the MAC layer, Internet Protocol version 4 (IPv4) and User Datagram Protocol (UDP) headers are all included in the calculation.

5.1.3 Overhead in Bytes

The average overhead in bytes is the total number of bytes transmitted in control messages divided by the total number of bytes in delivered data packets [121,122]. In wireless communications, the overhead in the MAC layer is calculated per transmission, therefore, few large transmissions lead to less total overhead than many small transmissions. As consequence, a high overhead in bytes is more tolerable than a high overhead in packets.

5.1.4 End-to-end Delay

The end-to-end delay of a packet is the amount of time that passes between its sending time and its receiving time [121,122]. For each simulation run, this value is then averaged over all packets that were actually received in this run. Packets that get dropped during the simulation period are not considered in this measure, because a dropped packet's delay would be infinite and make the measure useless. For brevity, the delay refers to the end-to-end delay from now on, whenever not explicitly states otherwise.

5.1.5 Robustness

The value of robustness is in the range of $[0, 1]$, with low values indicating that the black hole attack can disturb communication in the network to a high degree, while high values indicate a more resilient network. In order to calculate this parameter, the following formula is employed:

$$\text{Robustness} = 1 - \frac{\text{\# dropped packets due to attack}}{\text{\# delivered data packets}}$$

The first four measures presented in this section are used to quantify the effectiveness of the approach in solving the general problem it has been designed to address. Having a high PDR and a low delay measure with low or reasonable overhead would show that SAFEACO is suitable as a routing algorithm in general. The last measure quantifies the resistance against malicious attacks which aims for the packet drop.

5.1.6 Analytic Measures

In order to quantify the fluctuation of the metrics in the experimental results, the maximum variation $\text{Variation}_{\text{Max.}}$ and the standard deviation V_{Dev} are applied in the following sections. This first value is the difference between the maximum value $\text{V}_{\text{Max.}}$ and minimum value $\text{V}_{\text{Min.}}$ of a metric, as shown in the following equation:

$$\text{Variation}_{\text{Max.}} = \text{V}_{\text{Max.}} - \text{V}_{\text{Min.}}$$

For example, in table 5.3 the maximum PDR of SAFEACO-2BH is in scenarios when the maximum node speed is 5 m/s and the minimum PDR of SAFEACO-2BH is in scenarios when the maximum node speed is 30 m/s. Therefore, the maximum variation of of SAFEACO-2BH's PDR is the difference between these two PDR values. All other variation values used in this thesis are calculated in the same way.

The standard deviation V_{Dev} is a measure of how widely these metric values are dispersed from their mean values.

$$V_{Dev} = \sqrt{\frac{\sum_{i=1}^{N}(V_i - V_{mean})^2}{N}} \tag{5.1}$$

where V_{i} is the value of a metric; V_{mean} is the average value of that metric; N is the number of sample values of that metric.

To collect the data, ten runs of the simulation for each scenario with different random seeds are performed. Therefore, the final results shown in the figures are averaged based on the ten runs.

5.2 Performance Evaluation in MANETs

In order to comprehensively investigate the performance of SAFEACO, various of experiments based on different scenarios are launched. As introduced in section 2.4, two kinds of attacks are implemented in this series of experiments and the performance of SAFEACO is evaluated respectively for each attack. For the black hole attack scenarios, the maximum node speed and the number of CBR sessions are varied in the experiments. The number of Sybil nodes in the network and the number of Sybil identities per Sybil node are varied in the Sybil attack scenarios. Table 5.1 gives an overview of the different series of experiments launched in MANET scenarios.

Table 5.1: MANET experiments

MANET Experiments	
Black hole attacks	MANET series 1: varying max. node speed from 5 to 30 m/s MANET series 2: varying no. of CBR sessions from 5 to 10
Sybil attacks	MANET series 3: varying no. of Sybil nodes from 1 to 10 MANET series 4: varying no. of Sybil identities from 2 to 9

5.2.1 Performance Under Black Hole Attacks

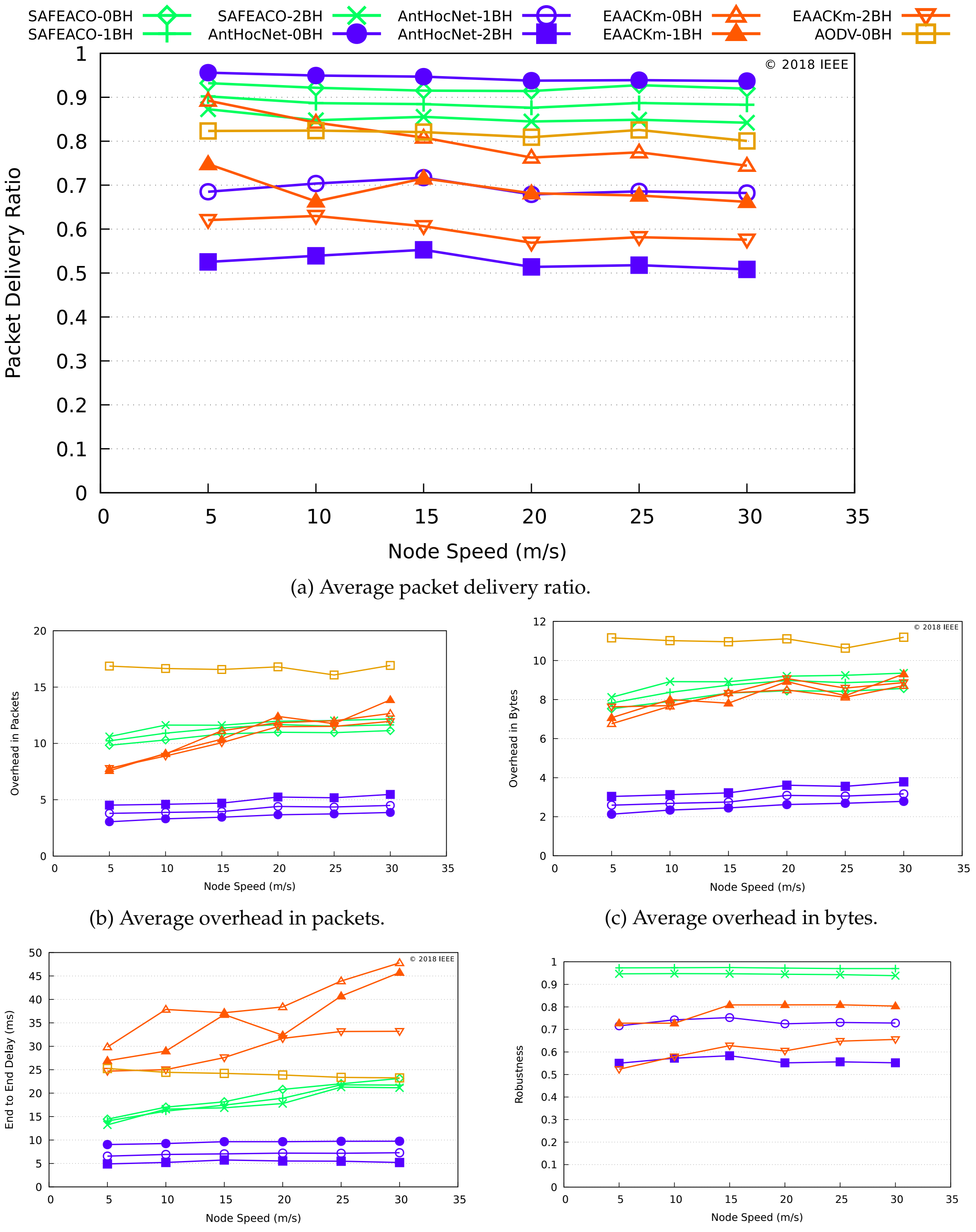
Under Black Hole Attack, Varying Node Speed

Starting from the basic scenario described in section 4.2.1, the maximum speed of the nodes is varied between $5\,\mathrm{m/s}$ and $30\,\mathrm{m/s}$ in $5\,\mathrm{m/s}$ steps. Since the aim is to evaluate the performance of SAFEACO in both normal and sophisticated environments, SAFEACO is simulated in three kinds of scenarios: without black hole attacks, with one ongoing black hole node and with two ongoing black hole nodes. AntHocNet and EAACKm are chosen for comparisons in different scenarios. Since AODV is one of the most representative state-of-the-art routing protocol in MANETs, its performance of in scenarios without any attacks is also demonstrate here as a baseline in the evaluation figures. The abbreviations used in the evaluation figures in this section can be found in table 5.8.

In theory, the topology of the network changes more frequently while the mobility of nodes increases. In consequence, links would break more often than in a network with low mobility nodes. Generally speaking, link breakages lead to more overhead, lower PDR and higher delay. For example, if a link which is involved in an active route breaks, the routing protocol should react to this change. Normally route error messages are sent out which causes more overhead and the intermediate nodes may try to find an alternative route to salvage the data packets affected by

Abbreviation	Description
AODV-0BH	AODV without black hole
AntHocNet-0BH	AntHocNet without black hole
AntHocNet-1BH	AntHocNet with 1 black hole
AntHocNet-2BH	AntHocNet with 2 black holes
EEACKm-0BH	EEACKm without black hole
EEACKm-1BH	EEACKm with 1 black hole
EEACKm-2BH	EEACKm with 2 black holes
SAFEACO-0BH	SAFEACO without black hole
SAFEACO-1BH	SAFEACO with 1 black hole
SAFEACO-2BH	SAFEACO with 2 black holes

Table 5.2: Abbreviations of different MANET configurations



(a) Average packet delivery ratio.

(b) Average overhead in packets.

(c) Average overhead in bytes.

(d) Average end-to-end delay.

(e) Average robustness.

Figure 5.1: Under black hole attack, varying node speed.

the link breakage. If the intermediate nodes successfully find a new route, they can forward the buffered data packets to the destination nodes; otherwise, the buffered packets will be dropped. This leads to a lower PDR. The salvaged data packets also cause a higher delay, due to the buffer time at the intermediate nodes.

Figure 5.1a [121] shows the simulation results for the PDR of SAFEACO, AntHocNet and EAACKm while the maximum node speed is increasing. AODV without attacks is provided as an anchor value for the performance comparison. Figure 5.1a shows that AntHocNet has the best performance of PDR in scenarios without any attacks and SAFEACO outperforms EAACKm and AODV obviously in this case. However, if there is any black hole nodes in the network, AntHocNet suffers more than the other two protocols and SAFEACO turns to be the best solution. Although a clear performance drop which caused by the black hole nodes can be found in all three protocols when the number of black hole nodes in the network increases, AntHocNet with a average drop of PDR in 41.8 % suffers the most, while the PDR of EAACKm drops 20.7 % in average. In comparison to them, SAFEACO with a drop in 7.0 % performs the best. Moreover, when focus on varying the node speed, the PDR of SAFEACO remains in the same level and above that of all other approaches under consideration in all scenarios under black hole attacks. On the contrary, the PDR of EAACKm under black hole attacks decreases while the node maximum speed increases. Looking at the differences in PDR over varying speeds, it is found that SAFEACO runs have lower variation in performance than EAACKm runs. Detailed variation data can be found in table 5.3. Overall, the PDR of SAFEACO is more stable and resilient against attacks than that of EAACKm.

Figure 5.1b and 5.1c [121] present the average overhead in packets and in bytes for all the selected protocols. A moderate growth in overhead for all protocols can be found in both figures, as is expected with growing speed. The overhead of SAFEACO both in packets and in bytes is higher than the one of AntHocNet in two cases. This is because in SAFEACO normal nodes which drop the data packets due to congestion would be classified as unreliable nodes. Due to this kind of misclassification, source nodes have to send new FANTs to discover new routes which leads to sending out more control packets. Therefore, SAFEACO has higher overhead than AntHocNet. Similar to SAFEACO, in EAACKm source nodes send out their own special control packets to detect the malicious nodes in the network and therefore it also has higher overhead than

Scenario	**Maximum variation**
SAFEACO-0BH	0.017918
SAFEACO-1BH	0.025846
SAFEACO-2BH	0.030623
EAACKm-0BH	0.147799
EAACKm-1BH	0.086153
EAACKm-2BH	0.060689

Table 5.3: Maximum PDR variation over speeds

AntHocNet. However, the overhead of EAACKm is almost always in the same level as the one of SAFEACO and both of them are below the overhead of AODV. Comparing the overhead in normal scenarios with the one in scenarios under attacks shows that the overhead of SAFEACO increases when the number of black hole nodes increases. A similar trend can be found with EAACKm, but it has slight fluctuations. Table 5.4 shows the maximum overhead variation, which is the difference between maximum and minimum overhead. The maximum overhead variation of EAACKm both in packets and bytes is higher than the one of SAFEACO. This shows that the overhead of EAACKm increases more than the one of SAFEACO while the node speed is increasing.

The average end-to-end delay is given in figure 5.1d [121]. An increasing trend can be clearly recognized in both SAFEACO and EAACKm, as is expected with growing speed. However, the delay of EAACKm is obviously higher and increases more rapidly than the one of SAFEACO in all cases. The delay variations of AODV and AntHocNet are $-8.4\,\%$ and $7.6\,\%$ respectively. Compare to $53.4\,\%$, the one of EAACKm, the delay of AODV and AntHocNet can be considered to remain in the same level when the node speed increases. Figure 5.1d shows that the ACO-based routing mechanisms outperform AODV routing approach. Although AntHocNet has the lowest delay, specially under black hole attacks, this is mainly an artifact of how delay is calculated in the experiments, where the delay caused by dropped packets is not considered. Figure 5.1a shows that AntHocNet lost the most data packets under the black hole attacks. When the number of black hole nodes in the network increases, the delay metric of the protocols decreases. For example, the delay of EAACKm-2BH is obviously lower than the one of EAACKm-0BH for all node speeds. One possible reason for this trend is that dropped packets are not considered during the calculation of delay. Figure 5.1a shows that more packets are dropped due to the black hole attack in AntHocNet-2BH, SAFEACO-2BH and EAACKm-2BH. Therefore, all protocols perform better with respect to average delay when they are attacked. Looking at the delay measurements of SAFEACO as speed goes up, it shows that delay increases slightly with increasing speed. EAACKm's delay is consistently much higher than that of SAFEACO in all considered cases.

Scenario	**Overhead in packets**	**Overhead in bytes**
SAFEACO-0BH	1.305850	1.040830
SAFEACO-1BH	1.450000	1.151830
SAFEACO-2BH	1.561700	1.236010
AntHocNet-0BH	0.822840	0.657380
AntHocNet-1BH	0.708780	0.578720
AntHocNet-2BH	0.952170	0.751890
EAACKm-0BH	4.911830	1.954427
EAACKm-1BH	6.298320	2.238928
EAACKm-2BH	4.157792	1.449652
AODV-0BH	0.850100	0.558200

Table 5.4: Maximum overhead variation over speeds

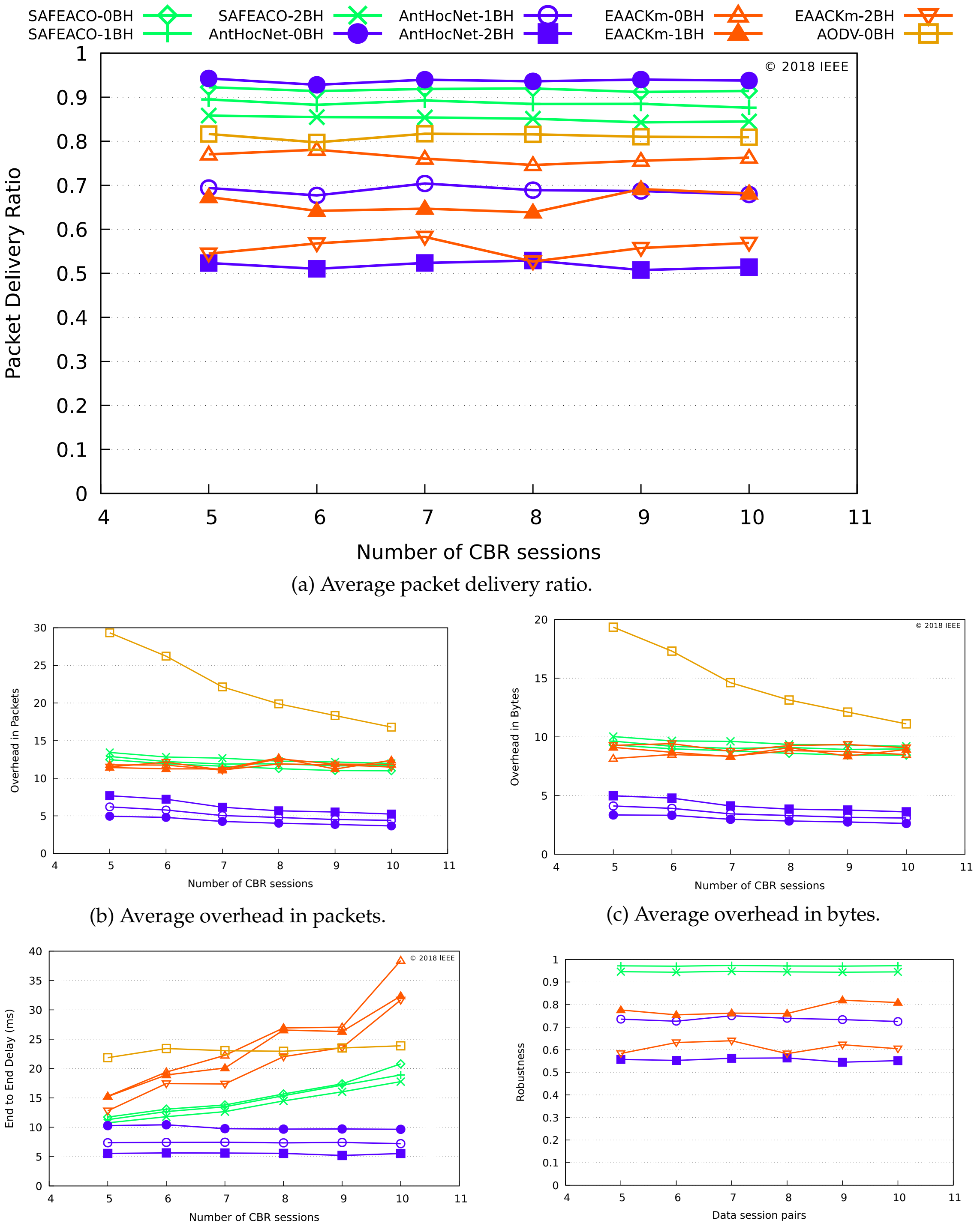
Figure 5.1e shows clearly that more black hole nodes bring more harmful effects to the network. However, unlike the AntHocNet and EAACKm, in which the effect of a second black hole node is obviously more pronounced, the robustness of SAFEACO reduces only slightly with two black hole nodes. AntHocNet doesn't have a direct defense mechanism against the black hole attacks, thus it is reasonable for it to have lower robustness values than SAFEACO. Although the robustness of EAACKm improves smoothly as node speed increases, the improvement is very limited. When the node speed is slow, its robustness is not better, in some cases, even worse than the robustness of AntHocNet. Moreover, the robustness of SAFEACO is not strongly affected by increasing node speeds. With both one and two black hole nodes, the performance of SAFEACO remains on a similar level and steadily above that of EAACKm and AntHocNet. From this point of view, SAFEACO is the best solution for defending the network against black hole attacks.

Under Black Hole Attack, Varying Number Of CBR Sessions

Starting from the basic scenario, the number of CBR sessions in this series of experiments is varied from 5 to 10. AntHocNet and EAACKm are chosen for comparisons in different scenarios. The performance of AODV in scenarios without any attacks is also demonstrated here as a baseline in the evaluation figures. The abbreviations used in the evaluation figures in this section are the same as shown in table 5.8.

In theory, the density of packets for network communication increases while the number of CBR sessions increases. In consequence, packet congestions would happen more often than in a network with low packets density. Packet congestions usually lead to retransmission of packets which further results in longer end-to-end delay. Moreover, in the worst case a high frequency of packet congestions could also result in dropping the packets which have exceeded their maximum retransmission times. Therefore, PDR could be reduced when the number of CBR sessions increases.

Figure 5.2 [126] shows various performance measures of SAFEACO, AntHocNet, EAACKm and AODV. When the number of CBR sessions increases, the PDR for all protocols almost remains at the same level. With the exception of EAACKm, the standard deviations of other lines are all under 0.8 %. The standard deviations of EAACKm in three scenarios are from 0.9 to 2.0 %. Generally speaking, the increase of CBR sessions leads to a slightly lower PDR as expected. However, the reduction in PDR is not huge in all considered cases. In scenarios without any black hole attacks, AntHocNet-0BH has the best PDR performance, but the difference between AntHocNet and SAFEACO is very small and both of them obviously outperforms the other two protocols. However, in scenarios with black hole attacks, AntHocNet suffers much more than the other two protocols and SAFEACO shows the best performance. Furthermore, the PDR decreases when there are more black hole nodes in the network. Although EAACKm outperforms AntHocNet when there are two black hole nodes in the network, in scenarios with one black hole node, EAACKm



(a) Average packet delivery ratio.

(b) Average overhead in packets.

(c) Average overhead in bytes.

(d) Average end-to-end delay.

(e) Average robustness.

Figure 5.2: Under black hole attack, varying number of CBR sessions.

performs generally worse than AntHocNet.

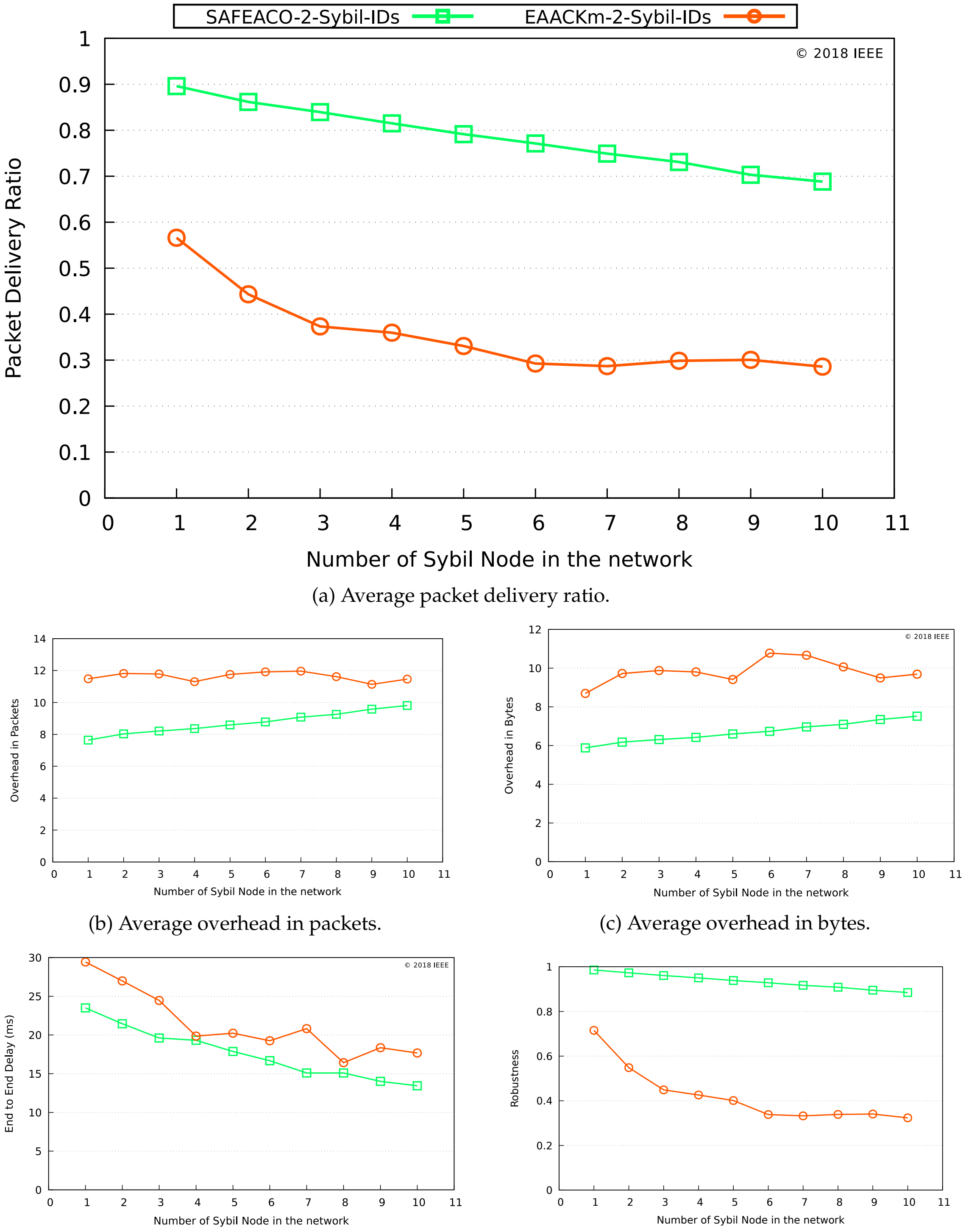
As shown in figure 5.2b and 5.2c [126], other than for EAACKm a clear dropping trend for the two kinds of overhead parameters can be found for all three remaining protocols. Despite AODV having the highest decrease in overhead, overall it remains the highest. In contrast, AntHocNet shows the lowest overhead in both cases. This indicates that the ACO routing structure works more efficiently when there is more communication traffic in the network. The same effect could also be seen for SAFEACO. However, the variation of overhead in SAFEACO is not as much as in AntHocNet. Another clear trend is that the two kinds of overhead increase when the number of black hole nodes increases. Instead of dropping, the overhead of EAACKm both in packets and in bytes stay almost at the same level. However, there are small fluctuations in both cases and the effect of the increased number of black hole nodes is not as clear for EAACKm as for the ACO-based routing protocols.

An increasing trend in the average end-to-end delay can be clearly recognized for SAFEACO, AODV and EAACKm, when the number of CBR sessions increases. With the rapid increase rate, the delay of EAACKm is obviously higher than that of SAFEACO and the difference between them is getting growing. Similar to figure 5.1d, AntHocNet in figure 5.2d [126] has the lowest delay, but this is mainly because the delay caused by dropped packets is not considered in the calculation. Figure 5.2a shows that AntHocNet loses the most data packets while under black hole attacks.

As previously seen in figure 5.1e, the robustness of SAFEACO under black hole attack in figure 5.2e is the best and it obviously outperforms other two protocols. It shows obviously that more malicious nodes bring more harmful effects to the network. However, the negative effect dose not reduce the robustness in SAFEACO much, unlike in AntHocNet and EAACKm. Although the robustness of EAACKm improves smoothly when there are more CBR sessions in the network, the improvement is limited and with fluctuations which might be caused by the authentication process designed in the original EAACK protocol.

5.2.2 Performance Under Sybil Attacks

This section presents the performance of SAFEACO under Sybil attacks which are introduced in section 2.4.2. Sybil attacks in which Sybil nodes only switch their identities do not bring harmful effect to the routing performance, so a black hole attack is embedded into the Sybil attack. In the following, Sybil attack refers to Sybil attacks with embedded black hole attacks, whenever not explicitly states otherwise. In theory this kind of Sybil attack is basically a variant of black hole attacks. However, it could give malicious nodes more opportunities to attack the network. For example, if the first identity is detected by the normal nodes, the Sybil node can switch its identity to another identity which is new in the network and the surrounding nodes will treat this identity as a new node.



(a) Average packet delivery ratio.

(b) Average overhead in packets.

(c) Average overhead in bytes.

(d) Average end-to-end delay.

(e) Average robustness.

Figure 5.3: Under Sybil attack, varying number of Sybil nodes.

Under Sybil Attack, Varying Number of Sybil Nodes

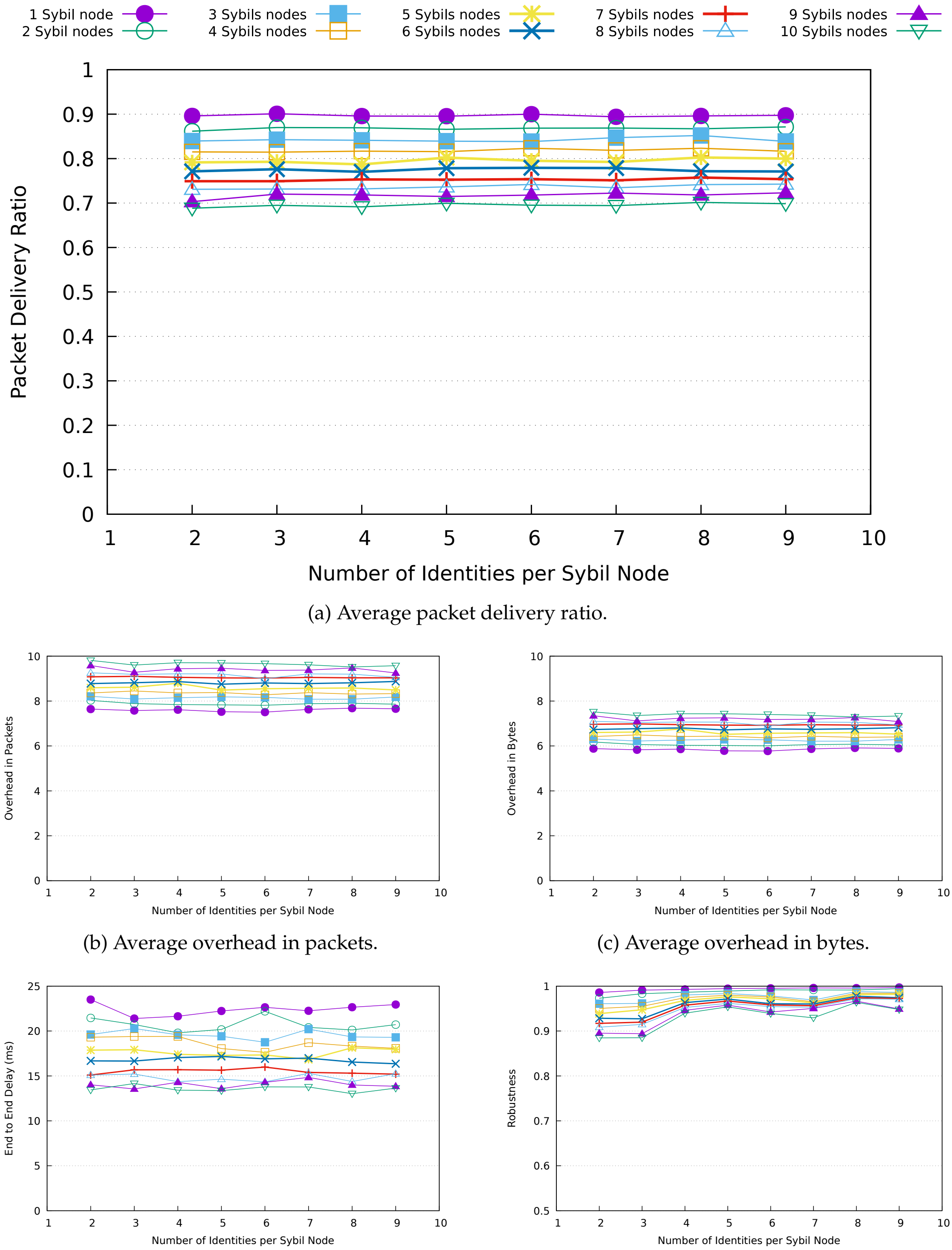
The base scenario used in this series evolved from the base scenario described in section 4.2.1. All parameters stay the same except that one node in the network is set to be the Sybil node which has two identities. The two identities are not shown simultaneously in the network, instead the Sybil node switches its identities in every 50 seconds and launches the black hole attack with each Sybil identity.

In order to investigate the performance of SAFEACO under Sybil attacks, the number of Sybil nodes in the network is increases from 1 to 10 and the results are presented in figure 5.3. Since the detailed investigation in section 5.2.1 shows that SAFEACO outperform AntHocNet obviously under black hole attack, in this series of experiments the performance of SAFEACO is only compared with that of EAACKm.

Figure 5.3a [121] shows that the PDR of both protocols decreases when the number of Sybil nodes increases. However, the PDR of SAFEACO is obviously higher than that of EAACKm. SAFEACO could deliver almost 70.0 % of the data packets even when 20.0 % of the network size are malicious, while EAACKm could only deliver ca. 30.0 % data packets under the same condition. Figure 5.3b and 5.3c [121] present the average overhead in packets and in bytes respectively. A moderate increase trend of SAFEACO is shown in both figures. However, the overhead of SAFEACO is still lower than that of EAACKm in both cases. Figure 5.3d [121] shows that the end to end delay of both protocols decreases when the number of Sybil nodes in the network increases. This tendency is probably due to way of the average end to end delay is calculated. As introduced in section 5.1, the delay caused by the dropped data packets is not considered in the calculation. Figure 5.3a shows that the percentage of dropped data packets is getting higher while the number of Sybil nodes is increasing. Figure 5.3e shows that more Sybil nodes bring more harmful effects to the network. With a drop of 39.2 % in robustness for EAACKm, the negative effect is more pronounced. However, this effect is smaller in SAFEACO which has a drop of 10.1 % instead. This indicates that SAFEACO is more robust than EAACKm under Sybil attacks.

Under Sybil Attack, Varying Number of Sybil identities

Starting from the base scenario described in section 4.2.1, all parameters stay the same except setting one node in the network to be the Sybil node which has multiple identities. These multiple identities are not shown simultaneously in the network, instead the Sybil node switches its identities every 50 seconds and launches the black hole attack with each Sybil identity. Different from the previous experiments, the number of Sybil identities which a Sybil node could have is increased from 2 to 9. Since the previous series of experiments shows that SAFEACO clearly outperform EAACKm under Sybil attacks, this series of experiments is designed only to investigate whether the Sybil attack against SAFEACO could become more effective with more Sybil identities.



(a) Average packet delivery ratio.

(b) Average overhead in packets.

(c) Average overhead in bytes.

(d) Average end-to-end delay.

(e) Average robustness.

Figure 5.4: Under Sybil attack, varying number of Sybil identities.

The results are presented in figure 5.4.

It's clear to see that when there are more Sybil nodes in the network, SAFEACO turns out to have lower PDR, higher overhead, lower delay and robustness and this tendency is clearly valid for all considered cases, no matter how many identities a Sybil node could have. When fixing the number of Sybil nodes in the network, the performance of SAFEACO remains at the same level when the number of Sybil identities increases. The fluctuations in PDR and in the two kinds of overhead are all under $0.6\,\%$ which is negligible. Although the delay of SAFEACO has more fluctuations, its standard deviation of delay is $2.2\,\%$ which is not huge. Another interesting finding is that the robustness value is getting slightly higher when the number of Sybil identities increases. The difference becomes easier to recognize when the number of Sybil identities is higher than three. A possible reason for this is that by switching its Sybil identities a Sybil node has to wait for new FANT packets to launch a black hole attack. Before receiving a new FANT packet with its new Sybil identity, the Sybil node can not drop any more packets. The total number of dropped packets is reduced and as consequence the robustness value is increased. However, the effect seen in the robustness value is not strictly dependent on the number of Sybil identities which is represented as small fluctuations in the figure. This might be due to randomness in the experiments and the growing trend in robustness can be clearly recognized.

Generally speaking, the results indicate that in SAFEACO Sybil nodes can not get more benefit by just increasing the number of Sybil identities. This is mainly because in SAFEACO each node estimates the reliability of its neighbor nodes based on their behavior in forwarding packets, not their identities. As soon as the output value from the fuzzy detection system is under the threshold value, the Sybil node will be considered as unreliable node, no matter which Sybil identity is currently in use. Therefore, in SAFEACO nodes can detect Sybil attacks efficiently.

5.2.3 Discussion

In this section, the performance of SAFEACO for MANET scenarios is investigated based on the different series of experiments. Two kinds of attacks are implemented to evaluate the performance. AODV, AntHocNet and EAACKm are chosen for the comparisons. Table 5.5 summarizes the comparison results. Instead of showing the two kinds of overhead separately, only one column for overhead is shown, since the variation trends of the two overhead metrics are identical. The results show that SAFEACO has the best PDR and highest robustness, although its overhead and delay are a little bit higher than AntHocNet. Despite this, SAFEACO is obviously the best solution when defending against black hole attacks. It's notable that AntHocNet has the lowest delay when considering only the received data packets. However, the PDR of AntHocNet is the lowest when under black hole attacks. In the two black hole nodes scenarios, the PDR of AntHocNet even drops to almost $50.0\,\%$ which makes the delay of AntHocNet less comparable. Moreover, the delay of SAFEACO is obviously lower than the one of EAACKm. Therefore, the fourth column of table 5.5

which is noted with (*), shows the second best protocol, SAFEACO, instead of AntHocNet.

Table 5.5: Best performance under black hole attacks

Varied Parameters	PDR	Overhead	Delay(*)	Robustness
Max. Node Speed	SAFEACO	AntHocNet	SAFEACO	SAFEACO
No. of CBR Sessions	SAFEACO	AntHocNet	SAFEACO	SAFEACO

Table 5.6: Performance of SAFEACO under Sybil attacks

Varied Parameters	PDR	Overhead	Delay	Robustness
No. of Sybil Nodes	decreased	increased	decreased	decreased
No. of Sybil Identities	stable	stable	stable	increased

Table 5.6 presents the tendency of SAFEACO's performance when varying the selected simulation parameters. It is clear that the performance of SAFEACO based on all evaluation metrics decreases when the number of Sybil nodes increases. However, when fixing the number of Sybil nodes in the network, but increasing the number of Sybil identities, the performance of SAFEACO is stable or even gets slightly better as is the case for robustness. This indicates that the malicious behavior detection system in SAFEACO works stably and efficiently, no mater how many identities a Sybil node has.

Overall, the simulation results show that SAFEACO is able to efficiently deliver the packets while dynamically detecting the malicious nodes in the network. The fuzzy based detection system robustly evaluates nodes based on limited information and has built-in high fault tolerance. The results of varying the maximum node speed experiments show that, the PDR performance of SAFEACO remains almost at the same level as the node speed increases. Specially, in comparison with other protocols, SAFEACO has the best PDR performance under black hole attacks. Moreover, SAFEACO also shows clearly better performance and robustness with its higher PDR and lower delay and overhead than EAACKm in scenarios with Sybil nodes.

In the next section, the performance and scalability of SAFEACO in different VANET scenarios will be further investigated.

5.3 Performance Evaluation in VANETs

In this section, various experiments are launched to investigate the performance of SAFEACO in VANET scenarios. As introduced in section 2.4, black hole and flooding attacks are implemented for this series of experiments and the performance of SAFEACO is evaluated respectively for each attack. Due to the new attack type, the fuzzy detection system is also modified as introduced in section 3.5.3. For the black hole attack scenarios, the number of black hole vehicles is varied from

1 to 5 in the experiments. The number of flooding vehicles in the network is also varied from 1 to 5 in the flooding attack scenarios. Finally, a series of experiments are launched, where black hole attacks and flooding attacks are simultaneous deployed in the network. Table 5.7 gives an overview of the different series of experiments launched in VANET scenarios.

Table 5.7: VANET experiments

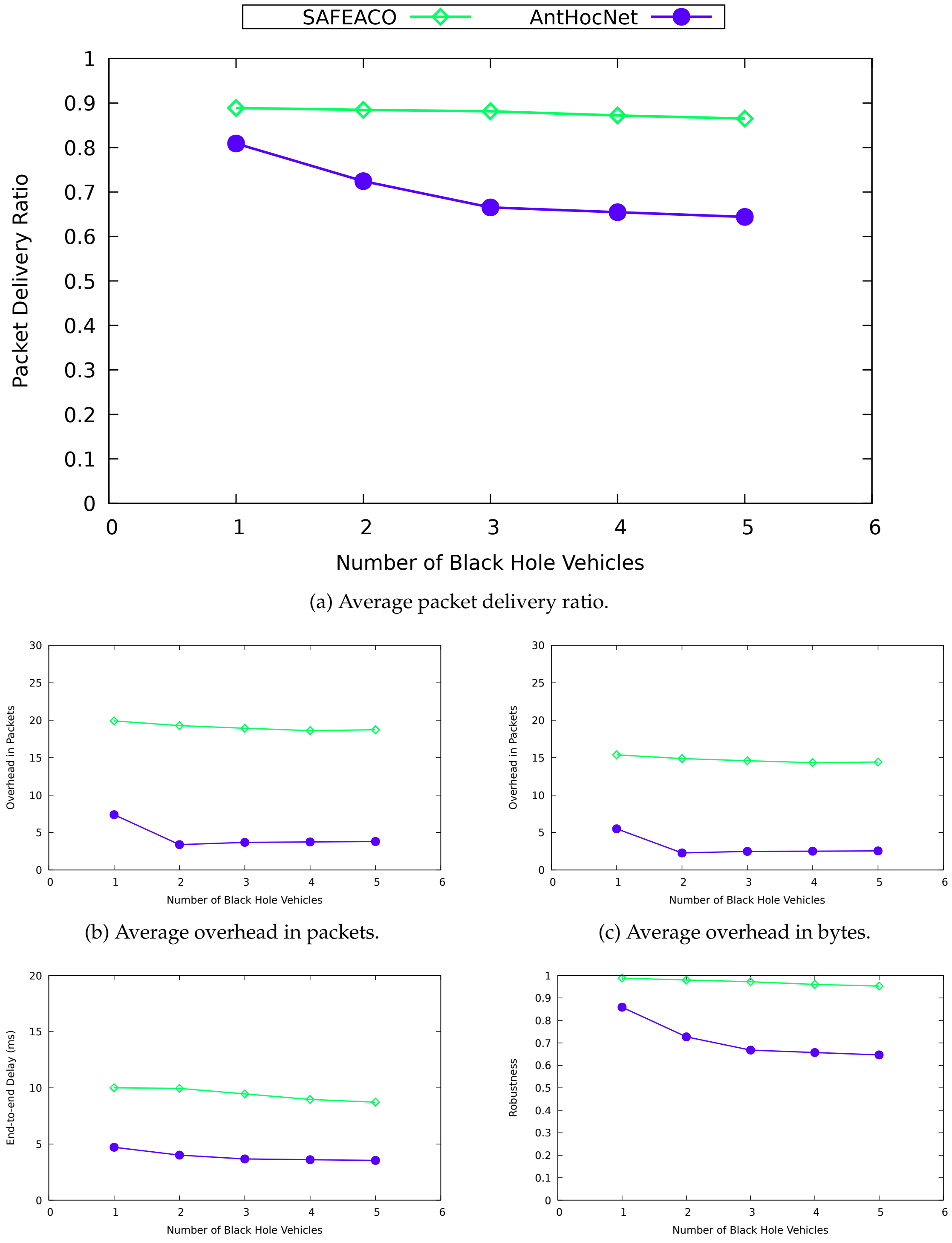
VANET Experiments	
Black hole attacks	VANET series 1: varying no. of black hole vehicles from 1 to 5
Flooding attacks	VANET series 2: varying no. of flooding vehicles from 1 to 5
Black hole or flooding attacks	VANET series 3: varying no. of total vehicles from 70 to 100
Black hole and flooding attacks	VANET series 4: varying no. of total vehicles from 70 to 100

5.3.1 Performance Under Black Hole Attacks

Starting from the basic scenario in section 4.3.1, the number of black hole vehicles in the network is increased from 1 to 5 to investigate the network performance of SAFEACO against the black hole attack over a range of different sophisticated scenarios. AntHocNet is chosen for comparisons in different scenarios.

In theory, more data packets will be dropped when there are more black hole vehicles in the network. Because the density of black hole vehicles is getting higher and the possibility that black hole vehicles receive the FANT packets is therefore increased. In consequence, PDR will be lower, while delay and overhead are experted to be higher.

Figure 5.5a shows that the PDR of both SAFEACO and AntHocNet drop as experted. However, the PDR of SAFEACO which has decreased by 2.4 % is obviously higher than that of AntHocNet which has decreased by 16.5 %. Specially, in a network with five black hole vehicles the PDR of SAFEACO still remains at 86.5 % while the PDR of AntHocNet is only 64.4 %. The overall average difference of PDR between the two protocols is 17.9 %. Despite the good performance in PDR, SAFEACO has higher overhead than AntHocNet as shown in figure 5.5b and 5.5c. Although the values are different, the trends in these two figures are identical. The results are similar as those in the series of MANET experiments. However, the overhead drops moderately in all cases when the number of black hole vehicles increases. This indicates that the ACO-based routing protocols have good reliability of overhead in the more sophisticated scenarios. In comparison with SAFEACO, the overhead of AntHocNet has higher fluctuations, especially when the number of black hole vehicles is increased from 1 to 2. This may be due to the randomness of the vehicles' positions. For example, in a scenario where two black hole vehicles block the source vehicle, the source vehicle could not find any route without attacks and all its data packets are dropped. After a while the reliability of these two vehicles is reduced under the threshold value and the source vehicle will not



(a) Average packet delivery ratio.

(b) Average overhead in packets.

(c) Average overhead in bytes.

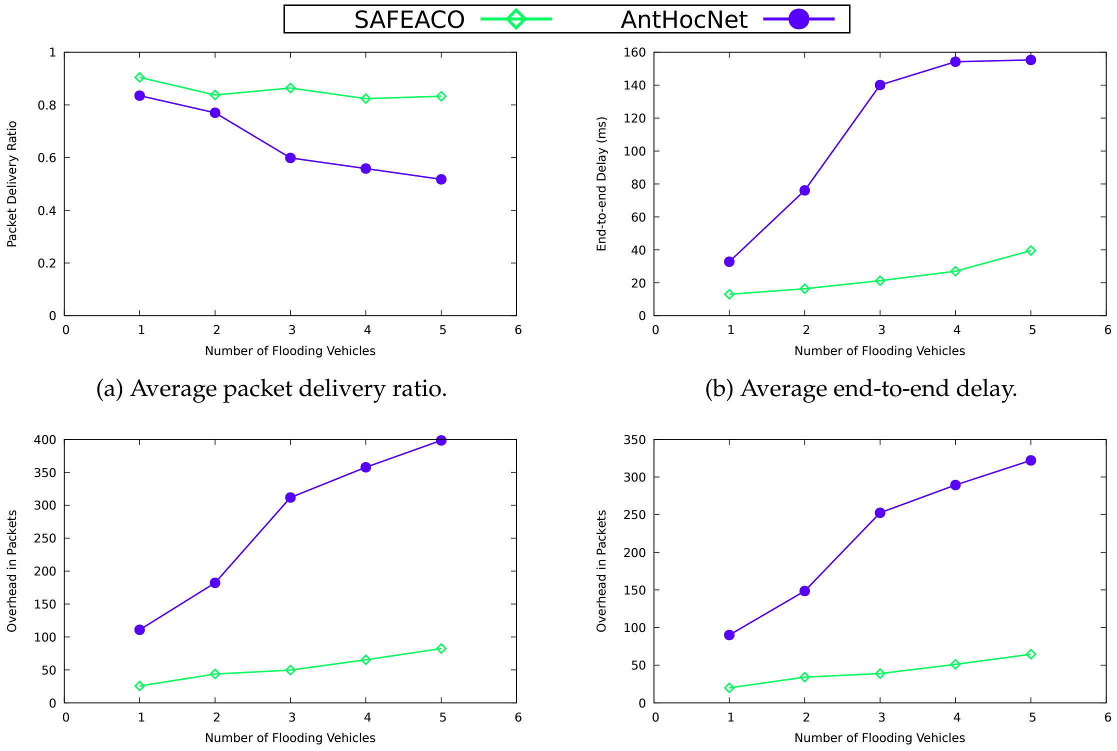
(d) Average end-to-end delay.

(e) Average robustness.

Figure 5.5: Under black hole attack, varying number of black hole vehicles.

consider them for packet transmission. As the source vehicle does not have any other neighbors, it will not send out further FANT packets to discover new routes. In consequence, the overhead in this scenario is reduced sharply. Besides the higher overhead, SAFEACO also has higher delay as shown in figure 5.5d. This trend is also similar to that in the MANET experiments. When there are more black hole vehicles in the network, the delay reduces moderately for both protocols. The explanation is the same as in the MANET scenarios. Figure 5.5e indicates that more black hole vehicles bring more harmful effects to the network. With a $21.2\,\%$ reduction of the robustness for AntHocNet, the negative effect is very pronounced. However, this effect is much smaller in SAFEACO which drops only by $3.5\,\%$, with an average robustness for SAFEACO of $97.1\,\%$. This indicates that SAFEACO can discover safe routes and deliver the packets more efficiently under black hole attacks.

5.3.2 Performance Under Flooding Attacks



(a) Average packet delivery ratio.

(b) Average end-to-end delay.

(c) Average overhead in packets.

(d) Average overhead in bytes.

Figure 5.6: Under flooding attack, varying number of flooding vehicles.

Starting from the basic scenario in section 4.3.1, the number of flooding vehicles in the network is increased from 1 to 5 to investigate the network performance of SAFEACO against the flooding attacks over a range of different sophisticated scenarios. AntHocNet is chosen for comparisons in different scenarios.

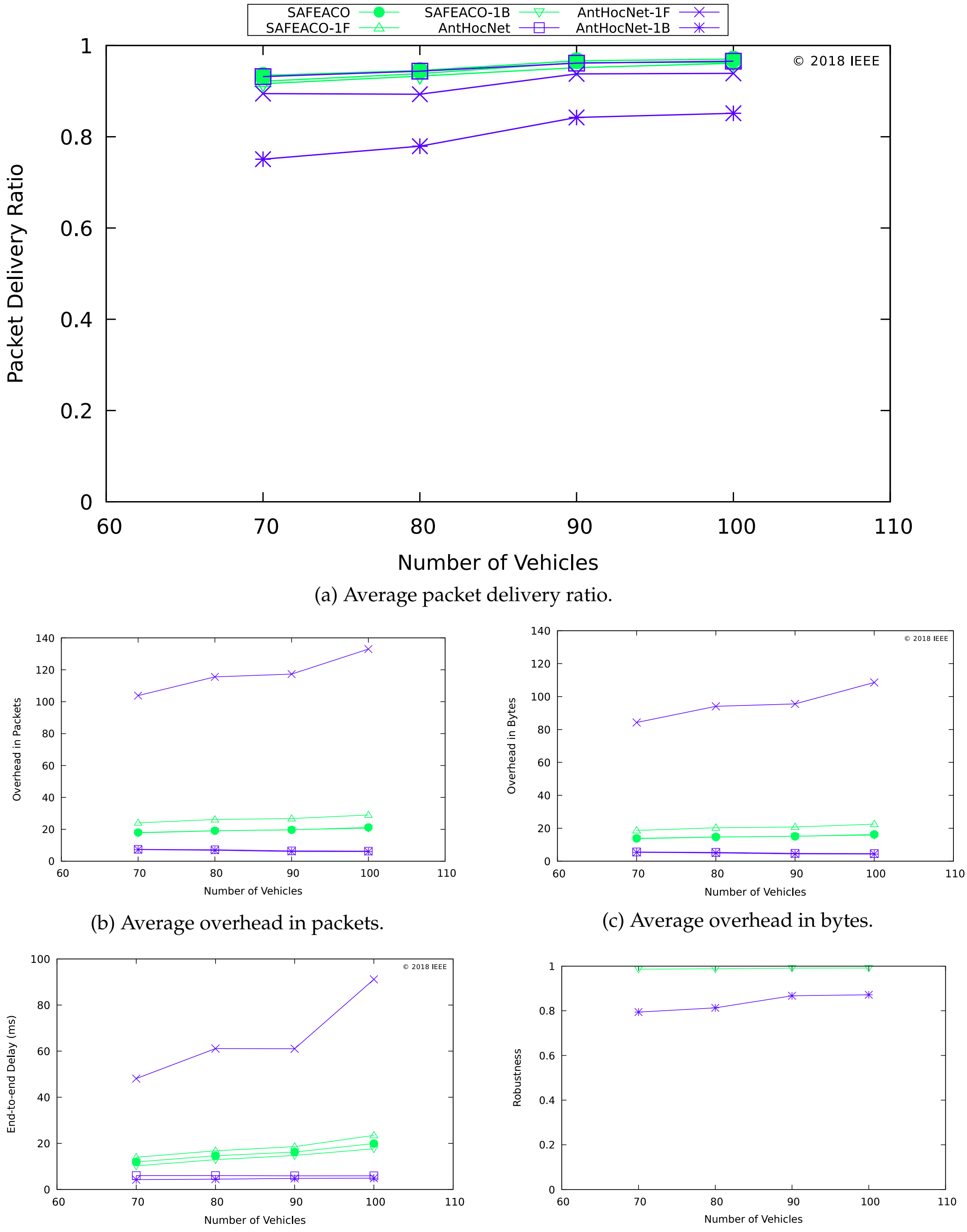
In theory, the flooding vehicles can block the wireless channel of their neighboring vehicles and maliciously induce the normal vehicles to search routes to the non-exist destination vehicles. The flooding attack aims to consume network resources, such as bandwidth, to exhaust the energy available to vehicles or their computational power and to disrupt the routing process in the network. Therefore, lower PDR, higher delay and overhead are expected in this series of experiments. One thing notable is that the performance metric "robustness" is not evaluated for any flooding attacks scenarios. If there is no packet drop attack in the network, then the robustness value will stay with 1 making it useless as a measure.

Figure 5.6 shows the results as expected. The PDR of SAFEACO drops moderately while the PDR of AntHocNet decreases more sharply. In the worst case, the PDR of AntHocNet is only $51.8\,\%$ while SAFEACO still remains at $83.3\,\%$. The negative effect caused by the flooding attack can be recognized also easily from the delay and the overhead. Figure 5.6b shows that AntHocNet suffers more significantly from the increased number of flooding vehicles. The lack of a malicious behavior detection system in AntHocNet leads to a rapid increase of delay. In the worst case, the delay of AntHocNet is almost four times the delay of SAFEACO. The same trend can be found in the two kinds of overhead. In the worst case, the overhead of AntHocNet is about five times the overhead of SAFEACO. All these results indicate that SAFEACO benefits from the fuzzy based detection system and that it can effectively defend against flooding attacks.

5.3.3 Performance As Vehicle Density Increases

In this section, the performance of SAFEACO in VANETs under both black hole and flooding attacks is investigated. Instead of running simulations with always 70 vehicles in the network, this series of experiments is launched in different scenarios which have different amounts of vehicles. Starting from the basic scenario, all parameters are kept the same, except for the number of vehicles. It is increased from 70 to 100, in steps of 10. This allows us to investigate network performance over a range of different vehicle density scenarios. SAFEACO is compared with AntHocNet under two kinds of attacks. The abbreviations used in the figures can be found in table 5.8.

In theory, the average number of neighbors per vehicle should increase as the vehicle density gets higher. In consequence, more alternative routes should exist between source and destination vehicles. In general, alternative routes improve the reliability of routing protocol against link breakages. For example, if a link which is involved in an active route breaks, the routing protocol could directly choose an alternative route and continue the data transmission. This increases the PDR. However, due to the higher vehicle density, there may exist more packet collisions which could lead to higher delay and overhead.



(a) Average packet delivery ratio.

(b) Average overhead in packets.

(c) Average overhead in bytes.

(d) Average end-to-end delay.

(e) Average robustness.

Figure 5.7: Under single type of attacks, varying number of vehicles.

The simulation results for SAFEACO and AntHocNet in three different scenarios each are shown in figure 5.7 [122]. It is clear that the PDR increases with the vehicle density in all cases. In the scenario without any attacks, the PDR of these both protocols is very close. However, if there is one malicious vehicle in the network, no matter if it is a black hole vehicle or flooding vehicle, the PDR of SAFEACO-1B and SAFEACO-1F turns out to be noticeably higher. With an average 17.5 % drop in the PDR AntHocNet suffers more when under black hole attacks, while the PDR of SAFEACO under both black hole and flooding attacks remains almost the same as in the case without any attacks.

Figure 5.7b and 5.7c [122] present the average overhead in packets and in bytes respectively. Since the tendency of the two kinds of overhead is the same, overhead in this section refers to the both kinds of overhead. With growing density a moderate growth of overhead can be found in all cases from these two figures. The overhead of AntHocNet-1F is obviously the highest one. This is mainly because of the flooded fake FANT packets and other control packets caused by these fake FANT packets. The overhead shown in figure 5.6c and 5.6d from the previous experiments also indicates that the flooding attack leads to higher overhead and delay. Other than AntHocNet-1F, the overhead of all other cases is stable and the overhead of the three SAFEACO cases is higher than AntHocNet and AntHocNet-1B. This is due to false positives of the fuzzy detection system. The system cannot differentiate packets dropped due to black hole attacks and those packets dropped due to regular channel issues, such as packet collisions. Once a normal vehicle is detected as a malicious vehicle, it will not be selected in any routes until it has proven that it is benign. This can cause a new route discovery process, which leads to additional overhead. The average end-to-end delay is given in figure 5.7d [122]. An increasing trend can be clearly recognized in both SAFEACO and AntHocNet when the network is attacked. But the increasing tendency of SAFEACO in delay is much more moderate in comparison to that of AntHocNet-1F. The delay of AntHocNet-1F is the highest in all cases. This indicates that the delay of AntHocNet suffers the most under the flooding attack. In normal cases, the delay of both SAFEACO and AntHocNet are stable. However, the delay value drops very slightly under black hole attack in SAFEACO-1B and AntHocNet-1B. This is mainly an artifact of how delay is calculated in the experiments, where the

Abbreviation	**Description**	**Section**
SAFEACO	SAFEACO without any malicious vehicle	section 5.3.3 & 5.3.4
SAFEACO-1B	SAFEACO with 1 black hole (BH) vehicle	section 5.3.3
SAFEACO-1F	SAFEACO with 1 flooding vehicle	section 5.3.3
SAFEACO-1B1F	SAFEACO with 1 BH & 1 flooding vehicle	section 5.3.4
AntHocNet	AntHocNet without any malicious vehicle	section 5.3.3 & 5.3.4
AntHocNet-1B	AntHocNet with 1 BH vehicle	section 5.3.3
AntHocNet-1F	AntHocNet with 1 flooding vehicle	section 5.3.3
AntHocNet-1B1F	AntHocNet with 1 BH & 1 flooding vehicle	section 5.3.4

Table 5.8: Abbreviations of different VANET configurations

delay caused by dropped packets is not considered. By looking to the PDR in figure 5.7a [122], it can be seen that SAFEACO-1B and AntHocNet-1B lost more data packets than the normal cases. Similar to the results presented in figure 5.1e, the robustness of SAFEACO-1B in figure 5.7e is obviously higher than the one of AntHocNet-1B. This indicates that SAFEACO can also protect the network against the black hole attack efficiently in VANET scenarios. Moreover, the robustness is increasing moderately while the number of vehicles is increasing which shows the reliability of SAFEACO in dense networks.

Overall, the results show that AntHocNet's PDR suffers a lot from black hole attacks and its delay and overhead suffers from flooding attacks. When using the AntHocNet routing protocol, either a black hole or a flooding vehicle can attack the network routing process very effectively. In contrast, the performance of SAFEACO is stable under both attacks. It does have higher delay or overhead in some cases, but its PDR is always better than that of AntHocNet when under attack. PDR, delay and overhead all increase with growing vehicle density.

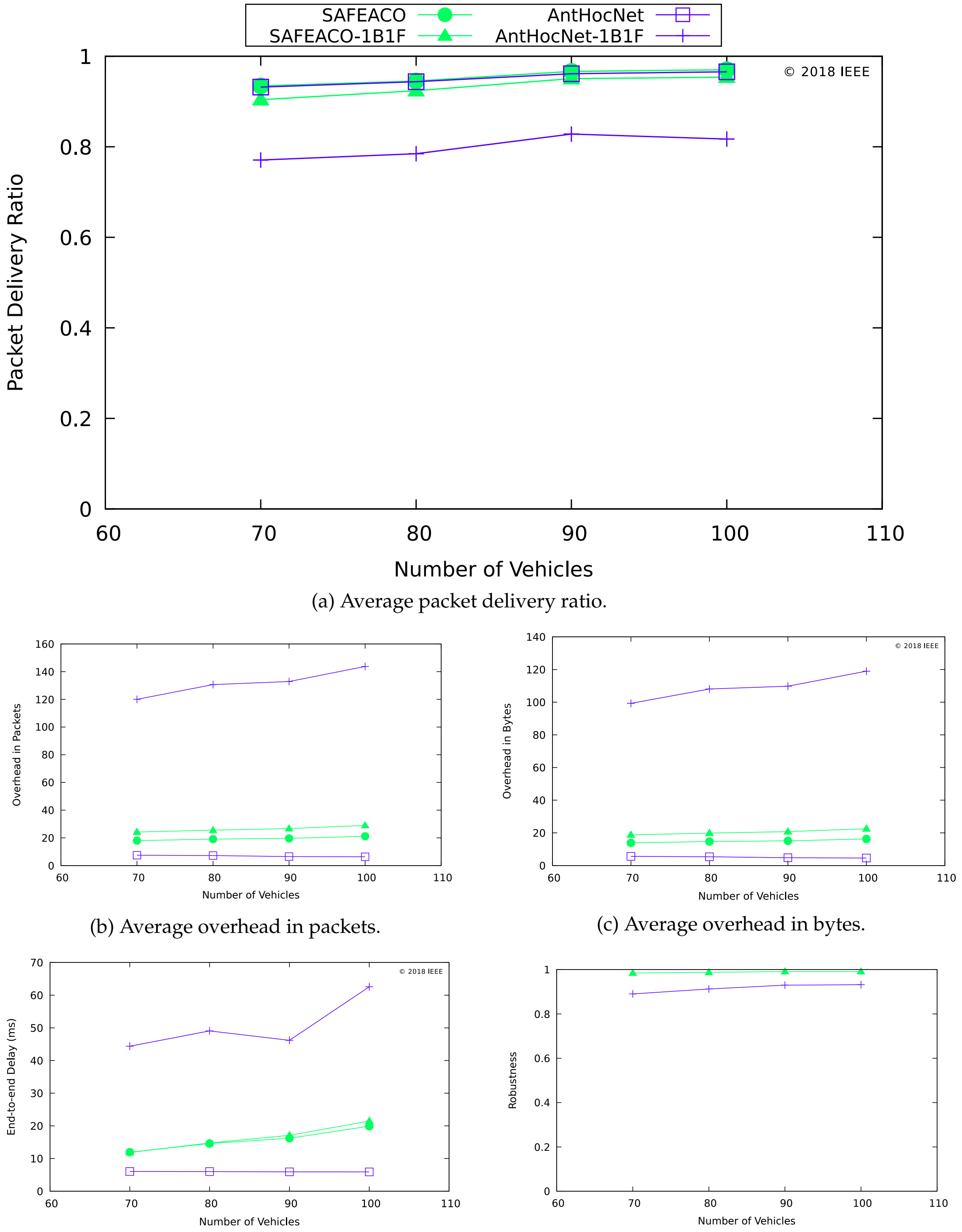
5.3.4 Performance Under Multiple Types of Attacks

This series of experiments is an extension of the previous series in section 5.3.3. All parameters used in this series of experiments are kept the same as the ones used in previous section. The scenarios with attacks however contain multiple attacks in the network at the same time. There are always two malicious vehicles: a black hole vehicle and a flooding vehicle. These two malicious vehicles work independently and do not collude with each other. SAFEACO is compared with AntHocNet under these concurrent types of attacks. The abbreviations used in the figures can be found in table 5.8.

Scenarios	**Reduction**
SAFEACO-1B	0.018056
SAFEACO-1F	0.012675
SAFEACO-1B1F	0.020987
AntHocNet-1B	0.180809
AntHocNet-1F	0.037155
AntHocNet-1B1F	0.150485

Table 5.9: Reduction of PDR in different scenarios

The simulation results are presented in figure 5.8 [122]. In scenarios without any malicious vehicle in the network, the PDR of SAFEACO and of AntHocNet is almost the same and it increases slightly when the vehicle density increases. However, SAFEACO outperforms AntHocNet in average by 0.3 % in this series of experiments. Table 5.9 shows the reduction of PDR between scenarios without any attacks and that with attacks. Comparing the PDR of SAFEACO with SAFEACO-1B1F, it shows a slight drop of 2.1 %. However, the drop of 15.0 % between AntHocNet and AntHocNet-1B1F is much more pronounced, showing its lower resilience against black hole



(a) Average packet delivery ratio.

(b) Average overhead in packets.

(c) Average overhead in bytes.

(d) Average end-to-end delay.

(e) Average robustness.

Figure 5.8: Under multiple types of attacks, varying number of vehicles.

and flooding attacks. The average overhead in packets and in bytes has the same trend as shown in figure 5.8b and 5.8c [122]. Therefore, overhead in this section refers to both kinds of overhead. A moderate growth of overhead can be found in all four cases. Here, the overhead of AntHocNet-1B1F is obviously higher than that of all other cases. The average end-to-end delay of AntHocNet-1B1F is the highest delay in figure 5.8d [122] which is similar to the delay of AntHocNet-1F in figure 5.7d [122]. This is mainly caused by the flooding attack. The delay of SAFEACO in both cases is higher than that of AntHocNet, with the same reason as mentioned in section 5.3.3. Similar to the results presented in figure 5.7e, the robustness of SAFEACO-1B1F in figure 5.8e is higher than the one of AntHocNet-1B1F. This indicates that SAFEACO performs well under both black hole and flooding attacks in VANET scenarios. Moreover, the increasing trend of robustness in this series of experiments indicates that the reliability of SAFEACO increases in dense networks.

Generally, the tendency of all the evaluation metrics in figure 5.7 is the same as the one in figure 5.8. Looking at the differences in PDR over varying vehicle density, it shows that high densities result in an increase in PDR. The same trend can be also found in the average end-to-end delay and the average overhead. However, there are some small differences. For example, the average delay of AntHocNet-1B1F is lower than that of AntHocNet-1F. This is mainly because the black hole attack caused a higher number of packets to be dropped and the delay of these dropped packets is not included in the calculation of the average delay. Moreover, the average overhead of AntHocNet-1B1F is higher than that of AntHocNet-1F in figure 5.7. This indicates that both the black hole and flooding attack can lead to higher overhead in AntHocNet. Nevertheless, the difference between the SAFEACO-1B1F and SAFEACO-1F is very small. This indicates that SAFEACO is resilient against black hole and flooding attacks and that this resilience still keeps increasing with increasing vehicle density when the number of malicious nodes in the network remains the same.

5.3.5 Discussion

In this section, the performance of SAFEACO for VANET scenarios is investigated based on the various series of experiments. Black hole and flooding attacks are applied to evaluate the performance of SAFEACO and AntHocNet. Table 5.10 summarizes the tendency of SAFEACO while increasing the number of malicious nodes in the network. Due to the identical trends, the third column in the table which is noted with (*) refers to the overhead in packets and the overhead in bytes. It is clear to see that the performance of SAFEACO gets worse in most of the cases when the number of malicious nodes increases. Looking at the results of scenarios with black hole attacks, the PDR of SAFEACO remains above $86.5\,\%$ even when there are five black hole nodes in the network and its overhead and delay also drop moderately when the number of black hole vehicles increases. This indicates that SAFEACO is resilient against black hole attacks. In contrast to the black hole attack scenarios, the overhead and delay increase in scenarios with flooding attacks when the number of flooding nodes increases. Moreover, the reduction in PDR is also high than the one in the black hole attack scenarios. This indicates that flooding attack is more harmful to the network than black hole attacks. However, SAFEACO clearly outperforms AntHocNet under flooding attacks. Overall, the PDR of SAFEACO is more stable and resilient against black hole attacks than that of AntHocNet and SAFEACO outperforms AntHocNet in PDR, overhead and delay when under flooding attacks.

Table 5.10: Trends of SAFEACO's performance under single attacks

Type of Attacks	**PDR**	**Overhead(*)**	**Delay**	**Robustness**
Black Hole	slightly reduced	reduced	reduced	slightly reduced
Flooding	moderately reduced	increased	increased	not evaluated

Table 5.11: Better performance under increasing vehicle density

Attack Types	**PDR**	**Overhead(*)**	**Delay**	**Robustness**
Black Hole (BH)	SAFEACO	AntHocNet	AntHocNet	SAFEACO
Flooding	SAFEACO	SAFEACO	SAFEACO	not evaluated
BH and Flooding	SAFEACO	SAFEACO	SAFEACO	SAFEACO

Table 5.11 summarizes the comparison results when varying vehicle density. Overhead as presented in this table again refers to both the overhead in packets and in bytes, since the trends of these metrics are identical. As explained in section 5.3.2, the robustness metric is not evaluated for scenarios with only flooding attacks. The comparisons show that SAFEACO outperforms AntHocNet in most of the cases under attacks. In scenarios with the black hole attacks, AntHocNet drops more data packets and therefore has a lower delay. However, AntHocNet still outperforms SAFEACO in overhead. It can be seen as a trade-off between overhead and security. Despite its higher overhead in scenarios with black hole attacks, SAFEACO is the better solution in sophisticated networks.

Overall, the simulation results show that SAFEACO can efficiently deliver the packets while dynamically detecting different types of malicious nodes in VANETs. The increased PDR in scenarios where the vehicle density increases also indicates that SAFEACO can adapt well to dense networks which are close to the urban scenarios in the daily life. Moreover, SAFEACO has obviously less overhead and delay than AntHocNet in scenarios with the flooding attacks. This is the result of the adapted fuzzy based detection system introduced in section 3.5.3. Besides black hole attacks, the detection system is also effective at recognizing flooding nodes in VANETs. The success of the adapted fuzzy based detection system also shows its general flexibility, which allows it to be adapted to handle any concrete demands of an application.

Chapter 6

Conclusion

In this chapter, the conclusion of this thesis will be presented and the possible research directions for the future work will also be discussed.

6.1 Summary

In this thesis SAFEACO [121, 122, 126] is proposed, which is a security aware fuzzy logic enhanced ant colony optimization based routing protocol for MANETs. SAFEACO is a hybrid routing approach which is inspired by the AntHocNet routing mechanism and it applies a distributed fuzzy logic detection system to exclude abnormal or malicious nodes from the routing process. SAFEACO applies the ACO algorithm to discover the optimal routes for efficient packet delivery. Meanwhile, the fuzzy logic based detection system dynamically updates the reliability ratings of nodes. This detection system robustly evaluates nodes based on limited network traffic information in the neighborhood collected by the nodes and has built-in high fault tolerance which can reduce misclassifications. For example, a normal node which has dropped a data packet due to packet collision will not be directly judged as malicious, because the detection system performs the evaluation based on the general behavior of nodes in a predefined period, not only on the dropping of a single packet. Moreover, the fuzzy reliability value will be updated dynamically, so normal nodes which are misclassified as malicious nodes still have a chance to prove themselves reliable by stably forwarding data packets.

The performance of SAFEACO is investigated in both MANET and VANET scenarios. Various experiments are launched as shown in table 5.1 and 5.7 from chapter 5 and three well-known network attacks introduced in section 2.4 are implemented to test the resilience of SAFEACO in sophisticated environments. The simulation results of the various experiments show that, SAFEACO scales well in different MANET and VANET scenarios and that it enables efficient routing by providing high PDR and low or comparable end-to-end delay and overhead.

Besides the efficient routing performance, SAFEACO also shows its resilience in defending against different types of network layer attacks. The robustness metric shows its high robustness against black hole, Sybil and flooding attacks. In addition, section 3.5.3 gives a good example for adapting the fuzzy logic based detection system to different scenarios. The experimental results show that SAFEACO can detect not only a single attack, such as black hole and flooding attacks, but it also can detect multiple attacks which are launched in the same time by different malicious nodes which do not collude with each other. Moreover, the corresponding modification in the detection system can be performed in two steps. Therefore, the SAFEACO routing protocol can be adapted further to provide higher efficiency and security in MANETs routing, according to different circumstances.

6.2 Future work

As the proposed SAFEACO is a initial research work in this area, the limitations and challenges in this work lead to further studies. In this section, a few of ideas, which are out of the scope of this thesis, but can be considered as the outset for future work, will be discussed briefly.

QoS Metrics

From the evaluation results, SAFEACO has shown its high efficiency in the routing process. However, until now it does not consider any QoS related routing metrics. In order to further improve the routing efficiency, some of the QoS metrics should be considered in the decision making for route selections. For example, adapting the equation 3.3 in section 3.1 to consider the remaining battery of a node and the bandwidth when estimating the cost for transferring packets. This extension does not change either the routing structure or the detection system and therefore can be easily adapted to SAFEACO.

Improving Security

Further improving the security level which SAFEACO can guarantee is a meaningful but challenging task. Regarding the security challenges in MANETs it would also be interesting to investigate the performance of SAFEACO under other types of attacks. In theory, the fuzzy logic based detection system should be able to defend against new types of attacks by performing the following two steps: First of all, metrics which are related to the targeted type of attacks should be identified and be added as new input values into the detection system. In the next step, the fuzzy rules used in the detection system need to be adapted according to these new input values. One such case is described in section 3.5.3. However, when the number of input values increases, it becomes more difficult to define the fuzzy rules, because fuzzy rules are usually made based on experience or opinions of experts and they may need to be adapted several times according to the application scenarios. Finding the proper way to select the input values for the detection system which will allow it to detect as many ongoing attacks as possible is an interesting future research direction of this work.

VANET Scenarios

Since VANET applications developed very fast in the recent years, there is a high demand for routing protocols which can provide secure and efficient communication in VANETs. Although SAFEACO has been investigated in some VANET scenarios and has shown good performance, these scenarios are based on an abstract map as shown in figure 4.1 in section 4.3.1. The streets in this map are parallel with each other and the distance between arbitrary adjacent traffic conjunctions is the same. However, this map is not very close to real urban environments in a city. Therefore, it is worthwhile to investigate the performance of SAFEACO in VANET scenarios with a real map. Another interesting series of research experiments is to compare the performance of SAFEACO in different VANET scenarios which have different area sizes with real maps. The results can indicate whether SAFEACO is resilient when the network size is varying. Furthermore, SAFEACO should be compared with other VANET routing protocols, such as the UMB [31] protocol.

Copyright Notice

Bibliography

[1] P. R. Center., "Spring 2017 survey." *The Statistics Portal, Statista*, 2018, accessed: Sep.12, 2018. [Online]. Available: http://www.pewglobal.org/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/

[2] M. Frikha, *Ad Hoc Networks: Routing, QoS and Optimization*. John Wiley & Sons, 2013.

[3] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless sensor networks*. Springer, 2006.

[4] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[5] J. Thomas, J. Robble, and N. Modly, "Off grid communications with android meshing the mobile world," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Nov 2012, pp. 401–405.

[6] O. Garden, "Firechat," accessed: Sep. 13, 2018. [Online]. Available: https://www.opengarden.com/firechat/

[7] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *ACM SIGCOMM computer communication review*, vol. 24, no. 4. ACM, 1994, pp. 234–244.

[8] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," Tech. Rep., 2003.

[9] D. B. Johnson, D. A. Maltz, J. Broch *et al.*, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, pp. 139–172, 2001.

[10] F. Dressler and O. B. Akan, "A survey on bio-inspired networking," *Computer Networks*, vol. 54, no. 6, pp. 881–900, 2010.

[11] G. Beni and J. Wang, "Swarm intelligence in cellular robotic systems," in *Robots and Biological Systems: Towards a New Bionics?* Springer, 1993, pp. 703–712.

[12] A. K. Kordon, "Swarm intelligence: The benefits of swarms," in *Applying Computational Intelligence*. Springer, 2010, pp. 145–174.

[13] E. Bonabeau, M. Dorigo, and G. Theraulaz, *Swarm intelligence: from natural to artificial systems*. Oxford university press, 1999, no. 1.

[14] J. Bishop, "Stochastic searching networks," in *Artificial Neural Networks, 1989., First IEE International Conference on (Conf. Publ. No. 313)*. IET, 1989, pp. 329–331.

[15] J. Kennedy and R. Eberhart, "Particle Swarm Optimization." IEEE, 1995, pp. 1942–1948.

[16] M. Dorigo, "Optimization, learning and natural algorithms," *Ph. D. Thesis, Politecnico di Milano, Italy*, 1992.

[17] M. Dorigo and T. Stützle, *Ant Colony Optimization*. MIT Press, Cambridge, 2004.

[18] H. Ahmed and J. Glasgow, "Swarm intelligence: concepts, models and applications," *School Of Computing, Queens University Technical Report*, 2012.

[19] J. Loo, J. L. Mauri, and J. H. Ortiz, *Mobile ad hoc networks: current status and future trends*. CRC Press, 2016.

[20] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," in *ACM SIGCOMM computer communication review*, vol. 24, no. 4. ACM, 1994, pp. 234–244.

[21] T. Clausen and P. Jacquet, "Optimized link state routing protocol (olsr)," Tech. Rep., 2003.

[22] Z. J. Haas, M. R. Pearlman, and P. Samar, "The zone routing protocol (zrp) for ad hoc networks," 2002.

[23] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "Eaack—a secure intrusion-detection system for manets," *IEEE transactions on industrial electronics*, vol. 60, no. 3, pp. 1089–1098, 2013.

[24] A. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, and H. Mouftah, "Aack: Adaptive acknowledgment intrusion detection for manet with node detection enhancement," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. IEEE, 2010, pp. 634–640.

[25] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," *IEEE transactions on mobile computing*, vol. 6, no. 5, 2007.

[26] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing oslr-based manet," *Ad Hoc Networks*, vol. 30, pp. 84–98, 2015.

[27] J. P. Macker and M. S. Corson, "Mobile ad hoc networks (manets): Routing technology for dynamic wireless networking," *Mobile Ad hoc networking*, vol. 9, pp. 255–273, 2004.

[28] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular technology magazine*, vol. 2, no. 2, 2007.

[29] B. Karp and H.-T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000, pp. 243–254.

[30] R. Santos, R. M. Edwards, A. Edwards, and D. Belis, "A novel cluster-based location routing algorithm for inter-vehicular communication," in *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, vol. 2. IEEE, 2004, pp. 1032–1036.

[31] G. Korkmaz, E. Ekici, F. Özgüner, and Ü. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, pp. 76–85.

[32] C. Maihofer, "A survey of geocast routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 2, 2004.

[33] H. Zhang, X. Wang, P. Memarmoshrefi, and D. Hogrefe, "A survey of ant colony optimization based routing protocols for mobile ad hoc networks," *IEEE Access*, vol. 5, pp. 24 139–24 161, 2017.

[34] C. S. Moreau, C. D. Bell, R. Vila, S. B. Archibald, and N. E. Pierce, "Phylogeny of the ants: diversification in the age of angiosperms," *Science*, vol. 312, no. 5770, pp. 101–104, 2006.

[35] B. Hölldobler and E. O. Wilson, *The ants*. Harvard University Press, 1990.

[36] G. F. Oster and E. O. Wilson, *Caste and ecology in the social insects*. Princeton University Press, 1978.

[37] T. Flannery, *Here on earth: a natural history of the planet*. Grove/Atlantic, Inc., 2011.

[38] C. Anderson, G. Theraulaz, and J.-L. Deneubourg, "Self-assemblages in insect societies," *Insectes sociaux*, vol. 49, no. 2, pp. 99–110, 2002.

[39] N. J. Mlot, C. A. Tovey, and D. L. Hu, "Fire ants self-assemble into waterproof rafts to survive floods," *Proceedings of the National Academy of Sciences*, vol. 108, no. 19, pp. 7669–7673, 2011.

[40] P. C. Foster, N. J. Mlot, A. Lin, and D. L. Hu, "Fire ants actively control spacing and orientation within self-assemblages," *Journal of Experimental Biology*, vol. 217, no. 12, pp. 2089–2100, 2014.

[41] N. Fujiwara-Tsujii, N. Yamagata, T. Takeda, M. Mizunami, and R. Yamaoka, "Behavioral responses to the alarm pheromone of the ant Camponotus obscuripes (Hymenoptera: Formicidae)," *Zoological science*, vol. 23, no. 4, pp. 353–358, 2006.

[42] F. Moyson and B. Manderick, *The collective behavior of ants: an example of self-organization in massive parallelism*. Artificial Intelligence Laboratory, Vrije Universiteit Brussel, 1988.

[43] S. Goss, S. Aron, J.-L. Deneubourg, and J. M. Pasteels, "Self-organized shortcuts in the Argentine ant," *Naturwissenschaften*, vol. 76, no. 12, pp. 579–581, 1989.

[44] M. Dorigo and L. M. Gambardella, "Ant colony system: a cooperative learning approach to the traveling salesman problem," *IEEE Transactions on evolutionary computation*, vol. 1, no. 1, pp. 53–66, 1997.

[45] B. Bullnheimer, R. F. Hartl, and C. Strauss, "A new rank based version of the Ant System. A computational study." 1997.

[46] V. Maniezzo, "Exact and approximate nondeterministic tree-search procedures for the quadratic assignment problem," *INFORMS journal on computing*, vol. 11, no. 4, pp. 358–369, 1999.

[47] T. Stützle and H. H. Hoos, "MAX–MIN ant system," *Future generation computer systems*, vol. 16, no. 8, pp. 889–914, 2000.

[48] C. Blum and M. Dorigo, "The hyper-cube framework for ant colony optimization," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 34, no. 2, pp. 1161–1172, 2004.

[49] D. W. Corne, A. Reynolds, and E. Bonabeau, "Swarm intelligence," in *Handbook of Natural Computing*. Springer, 2012, pp. 1599–1622.

[50] M. Dorigo, V. Maniezzo, and A. Colorni, "Ant system: optimization by a colony of cooperating agents," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 26, no. 1, pp. 29–41, 1996.

[51] G. Di Caro and M. Dorigo, "AntNet: Distributed stigmergetic control for communications networks," *Journal of Artificial Intelligence Research*, vol. 9, pp. 317–365, 1998.

[52] M. Gunes, U. Sorges, and I. Bouazizi, "ARA-the ant-colony based routing algorithm for MANETs," in *Parallel Processing Workshops, 2002. Proceedings. International Conference on*. IEEE, 2002, pp. 79–85.

[53] J. S. Baras and H. Mehta, "A probabilistic emergent routing algorithm for mobile ad hoc networks," in *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2003, pp. 10–pages.

[54] G. Di Caro, F. Ducatelle, and L. M. Gambardella, "AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks," *European Transactions on Telecommunications*, vol. 16, no. 5, pp. 443–455, 2005.

[55] I. Scalable Network Technologies, “QualNet simulator,” 2011, accessed: Dez. 18, 2018. [Online]. Available: https://web.scalable-networks.com/qualnet-network-simulator-software

[56] E. Osagie, P. Thulasiraman, and R. K. Thulasiram, “PACONET: imProved ant colony optimization routing algorithm for mobile ad hoc networks,” in *22nd International Conference on Advanced Information Networking and Applications (aina 2008)*. IEEE, 2008, pp. 204–211.

[57] W.-J. Yu, G.-M. Zuo, and Q.-Q. Li, “Ant colony optimization for routing in mobile ad hoc networks,” in *2008 International Conference on Machine Learning and Cybernetics*, vol. 2. IEEE, 2008, pp. 1147–1151.

[58] J. Wang, E. Osagie, P. Thulasiraman, and R. K. Thulasiram, “HOPNET: A hybrid ant colony optimization routing algorithm for mobile ad hoc network,” *Ad Hoc Networks*, vol. 7, no. 4, pp. 690–705, 2009.

[59] A. Kathirvel, *Introduction to GloMoSim*. LAP Lambert Academic Publishing, 2011.

[60] Z. J. Haas, M. R. Pearlman, and P. Samar, “The zone routing protocol (ZRP) for ad hoc networks,” 2002.

[61] S. Sethi and S. K. Udgata, “The efficient ant routing protocol for MANET,” *International Journal on Computer Science and Engineering*, vol. 2, no. 07, pp. 2414–2420, 2010.

[62] I. Park, J. Kim, and I. Pu, “Blocking expanding ring search algorithm for efficient energy consumption in mobile ad hoc networks,” in *WONS 2006: Third Annual Conference on Wireless On-demand Network Systems and Services*, 2006, pp. 191–195.

[63] O. Hussein and T. Saadawi, “Ant routing algorithm for mobile ad-hoc networks (ARAMA),” in *Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International*. IEEE, 2003, pp. 281–290.

[64] E. Khosrowshahi-Asl, M. Noorhosseini, and A. S. Pirouz, “A dynamic ant colony based routing algorithm for mobile ad-hoc networks,” *Journal of information science and engineering*, vol. 27, no. 5, pp. 1581–1596, 2011.

[65] P. V. Krishna, V. Saritha, G. Vedha, A. Bhiwal, and A. S. Chawla, “Quality-of-service-enabled ant colony-based multipath routing for mobile ad hoc networks,” *IET communications*, vol. 6, no. 1, pp. 76–83, 2012.

[66] A. D. Al-Ani and J. Seitz, “QoS-aware Routing in Multi-rate Ad hoc Networks Based on Ant Colony Optimization,” *Network Protocols and Algorithms*, vol. 7, no. 4, pp. 1–25, 2016.

[67] J. D. Case, M. Fedor, M. L. Schoffstall, and J. Davin, “Simple network management protocol (SNMP),” Tech. Rep., 1990.

[68] T. Back, *Evolutionary algorithms in theory and practice: evolution strategies, evolutionary programming, genetic algorithms*. Oxford university press, 1996.

[69] I. Woungang, M. S. Obaidat, S. K. Dhurandher, A. Ferworn, and W. Shah, "An ant-swarm inspired energy-efficient ad hoc on-demand routing protocol for mobile ad hoc networks," in *2013 IEEE International Conference on Communications (ICC)*. IEEE, 2013, pp. 3645–3649.

[70] S. Misra, S. K. Dhurandher, M. S. Obaidat, P. Gupta, K. Verma, and P. Narula, "An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks," *Journal of systems and software*, vol. 83, no. 11, pp. 2188–2199, 2010.

[71] P. Vijayalakshmi, S. A. J. Francis, and J. A. Dinakaran, "A robust energy efficient ant colony optimization routing algorithm for multi-hop ad hoc networks in MANETs," *Wireless Networks*, pp. 1–20, 2015.

[72] J. Zhou, H. Tan, Y. Deng, L. Cui, and D. D. Liu, "Ant colony-based energy control routing protocol for mobile ad hoc networks under different node mobility models," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, p. 1, 2016.

[73] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 2, March 2003, pp. 1312–1321 vol.2.

[74] S. B. Prabaharan and R. Ponnusamy, "Secure and energy efficient MANET routing incorporating trust values using hybrid ACO," in *2016 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2016, pp. 1–8.

[75] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements and Performance Second Edition*. Lincoln, MA: Ganga-Jamuna Press, 2006.

[76] H. Zhang, X. Wang, and D. Hogrefe, "A Survey of Location Aware Ant Colony Optimization Routing Protocols in MANETs," in *10th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*. EAI, 2017.

[77] S. Kamali and J. Opatrny, "Posant: A position based ant colony routing algorithm for mobile ad-hoc networks," in *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on*. IEEE, 2007, pp. 21–21.

[78] D. Kadono, T. Izumi, F. Ooshita, H. Kakugawa, and T. Masuzawa, "An ant colony optimization routing based on robustness for ad hoc networks with GPSs," *Ad Hoc Networks*, vol. 8, no. 1, pp. 63–76, 2010.

[79] S. L. O. Correia, J. Celestino, and O. Cherkaoui, "Mobility-aware ant colony optimization routing for vehicular ad hoc networks," in *2011 IEEE Wireless Communications and Networking Conference*. IEEE, 2011, pp. 1125–1130.

[80] M. Killat and H. Hartenstein, "An empirical model for probability of packet reception in vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 1, 2009.

[81] J. Härri, C. Bonnet, and F. Filali, "Kinetic mobility management applied to vehicular ad hoc network protocols," *Computer Communications*, vol. 31, no. 12, pp. 2907–2924, 2008.

[82] H. Rana, P. Thulasiraman, and R. K. Thulasiram, "MAZACORNET: Mobility aware zone based ant colony optimization routing for VANET," in *2013 IEEE Congress on Evolutionary Computation*. IEEE, 2013, pp. 2948–2955.

[83] J. Nzouonta, "Vehicular network movement generator," accessed: Jan.1,2011. [Online]. Available: http://web.njit.edu/~borcea/invent/

[84] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*. Springer Science & Business Media, 2011.

[85] S. Balaji, S. Sureshkumar, and G. Saravanan, "Cluster based ant colony optimization routing for vehicular ad hoc networks," *International Journal of Scientific & Engineering Research*, vol. 4, no. 6, pp. 26–30, 2013.

[86] M. H. Eiza, T. Owens, and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 32–45, 2016.

[87] V. Vijayalakshmi and T. Palanivelu, "Secure antnet routing algorithm for scalable adhoc networks using elliptic curve cryptography," *Journal of Computer Science*, vol. 3, no. 12, pp. 939–943, 2007.

[88] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic curve cryptography," *Ubiquity*, vol. 2008, no. May, p. 7, 2008.

[89] S. Mehfuz and M. Doja, "Swarm intelligent power-aware detection of unauthorized and compromised nodes in MANETs," *Journal of Artificial Evolution and Applications*, vol. 2008, p. 3, 2008.

[90] H. Krawczyk, R. Canetti, and M. Bellare, "HMAC: Keyed-hashing for message authentication," 1997.

[91] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002*, 2002, pp. 193–204.

[92] S. J. Mirabedini and M. Teshnehlab, "FuzzyAntNet: a novel multi-agent routing algorithm for communications networks," *GESJ: Comput. Sci. Telecommun*, vol. 12, no. 1, pp. 45–49, 2007.

[93] S. J. Mirabedini, M. Teshnehlab, and A. Rahmani, "FLAR: An Adaptive Fuzzy Routing Algorithm for Communications Networks Using Mobile Ants," in *Convergence Information Technology, 2007. International Conference on*. IEEE, 2007, pp. 1308–1315.

[94] S. J. Mirabedini, M. Teshnehlab, M. Shenasa, A. Movaghar, and A. M. Rahmani, “AFAR: adaptive fuzzy ant-based routing for communication networks,” *Journal of Zhejiang University Science A*, vol. 9, no. 12, pp. 1666–1675, 2008.

[95] M. Goswami, R. Dharaskar, and V. Thakare, “Fuzzy ant colony based routing protocol for mobile ad hoc network,” in *Computer Engineering and Technology, 2009. ICCET'09. International Conference on*, vol. 2. IEEE, 2009, pp. 438–444.

[96] S. Sethi and S. K. Udgata, “Fuzzy-based trusted ant routing (FTAR) protocol in mobile ad hoc networks,” in *International Workshop on Multi-disciplinary Trends in Artificial Intelligence*. Springer, 2011, pp. 112–123.

[97] G. Indirani and K. Selvakumar, “Swarm based Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks,” *International Journal of Computer Applications*, vol. 50, no. 19, 2012.

[98] K. Sowmya, T. Rakesh, and D. P. Hudedagaddi, “Detection and prevention of blackhole attack in MANET using ACO,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 12, no. 5, p. 21, 2012.

[99] S. Pal, K. Ramachandran, and S. Dhanasekaran, “A Review on Anomaly Detection in Manet Using Antnet Algorithm,” *Middle-East Journal of Scientific Research*, vol. 22, no. 5, pp. 690–697, 2014.

[100] P. Memarmoshrefi, H. Zhang, and D. Hogrefe, “Investigation of a bio-inspired security mechanism in Mobile Ad hoc Networks,” in *WiMob*, 2013, pp. 709–716.

[101] ——, “Social insect-based sybil attack detection in mobile ad-hoc networks,” in *Proceedings of the 8th International Conference on Bioinspired Information and Communications Technologies*, 2014, pp. 141–148.

[102] H. Zhang, P. Memarmoshrefi, F. Ashrafi, and D. Hogrefe, “Investigating the Learning Phase of an Autonomous Authentication in Mobile Ad-hoc Networks,” in *proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, 2016, pp. 91–92.

[103] O. Technologies, “OPNET,” 2003, accessed: Dez. 18, 2018. [Online]. Available: https://www.riverbed.com/de/products/steelcentral/opnet.html

[104] A. Varga *et al.*, “The OMNeT++ discrete event simulation system,” in *Proceedings of the European simulation multiconference (ESM'2001)*, vol. 9, no. S 185. sn, 2001, p. 65.

[105] G. F. Riley and T. R. Henderson, “The ns-3 network simulator,” in *Modeling and tools for network simulation*. Springer, 2010, pp. 15–34.

[106] S. M. Mousavi, H. R. Rabiee, M. Moshref, and A. Dabirmoghaddam, "Mobisim: A framework for simulation of mobility models in mobile ad-hoc networks," in *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007)*. IEEE, 2007, pp. 82–82.

[107] M. Liu, Y. Sun, R. Liu, and X. Huang, "An improved ant colony QoS routing algorithm applied to mobile ad hoc networks," in *2007 International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE, 2007, pp. 1641–1644.

[108] R. Barr, "SWANS User Guide," 2004, accessed: Dez. 18, 2018. [Online]. Available: http://jist.ece.cornell.edu/docs.html

[109] A. Nadeem and M. P. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013.

[110] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*. ACM, 2012, pp. 55–64.

[111] J. D. Day and H. Zimmermann, "The osi reference model," *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1334–1340, 1983.

[112] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005, pp. 46–57.

[113] R. Sokullu, O. Dagdeviren, and I. Korkmaz, "On the ieee 802.15. 4 mac layer attacks: Gts attack," in *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*. IEEE, 2008, pp. 673–678.

[114] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications magazine*, vol. 40, no. 10, pp. 70–75, 2002.

[115] S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in *proceedings of the world congress on engineering and computer science*, vol. 2008, 2008.

[116] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1976–1986.

[117] P. Yi, Z. Dai, S. Zhang, Y. Zhong *et al.*, "A new routing attack in mobile ad hoc networks," *International Journal of Information Technology*, vol. 11, no. 2, pp. 83–94, 2005.

[118] R. Gill, J. Smith, and A. Clark, "Experiences in passively detecting session hijacking attacks in ieee 802.11 networks," in *Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54*. Australian Computer Society, Inc., 2006, pp. 221–230.

[119] C. Siva, R. Murthy, and B. Manoj, "Ad hoc wireless networks: architectures and protocols," *Communications Engineering and Emerging Technologies Series*, 2004.

[120] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the mac layer in wireless ad hoc networks," in *MILCOM 2002. Proceedings*, vol. 2. IEEE, 2002, pp. 1118–1123.

[121] H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "A Security Aware Fuzzy Enhanced Ant Colony Optimization Routing in Mobile Ad hoc Networks," in *Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2018.

[122] ——, "A Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization Routing in Vehicular Ad hoc Networks," in *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2018, pp. 1071–1078.

[123] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

[124] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[125] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004, pp. 259–268.

[126] H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "Employing Fuzzy Logic to Provide Security Awareness in ACO Routing for MANETs," 2018.

[127] F. Ducatelle, "Adaptive routing in ad hoc wireless multi-hop networks," Ph.D. dissertation, Università della Svizzera italiana, 2007.

[128] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo-simulation of urban mobility," *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, 2012.

[129] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, 1946.