Trust Management for Security Enhancements in Ad hoc Networking Paradigms with Uncertain Reasoning

by

Zhexiong Wei

A thesis submitted to the

Faculty of Graduate Studies and Research

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering (OCIECE)

Department of Systems and Computer Engineering

Carleton University

Ottawa, Ontario, Canada, K1S 5B6

Oct, 2016

The undersigned hereby recommends to the

Faculty of Graduate Studies and Research

acceptance of the thesis

Trust Management for Security Enhancements in Ad hoc Networking Paradigms with Uncertain Reasoning

submitted by

Zhexiong Wei, **M.Eng**

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical and Computer Engineering

External Examiner, Professor Long Le, INRS

Thesis Supervisor, Professor F. Richard Yu,
Department of Systems and Computer Engineering

Carleton University

Octorber 2016

Abstract

Trust-based schemes are promising techniques to tackle inside attacks in distributed self-organized networks, such as mobile ad hoc networks and vehicular ad hoc networks. For the outside attackers, access control, authorization and authentication by cryptography can effectively thwart most of them. For the inside attackers, prevention based schemes such as cryptographic techniques are usually powerless. In the trust management system, trust is defined as the degree of belief that an entity can behave correctly in an observer's perspective. Compared to prevention-based schemes, detection-based schemes, such as trust management, dynamically estimate the internal nodes behavior. Based on the results of the estimation, the detection system makes the decision whether the node is a malicious attacker. These detection-based schemes introduce a large amount of uncertainties due to the unpredictable behavior of each node in the networks. Therefore, in the trust management system, accurate trust assessment is playing a key role in the trust management. It is significantly affected by uncertainty. In order to obtain accurate trust of each entity in the network, we apply uncertain reasoning, coming from the artificial intelligence field, to trust management in the emerging networking paradigms.

In this dissertation, we focus on trust management with the probability methodologies. This is because that Bayesian probability can formulate the trust in distributed self-organized networks better than rule-based schemes. Under the framework of uncertain reasoning, we adopt three approaches to evaluate trust accurately:

Bayesian inference, Dempster-Shafer theory (DST) and Bayesian networks model. We first consider the Mobile Ad hoc Network (MANET) environment with malicious insider attackers. We use the Bayesian inference method to assess the trust of nodes in MANETs based on the behavior of each node. Trust of each node is formulated by a posterior probability. In order to fully estimate trust, the DST is applied to calculate the trust with indirect observations. The system of trust management excludes the malicious nodes that have low trust values. We demonstrate that in the malicious scenarios the proposed schemes can outperform the existing schemes in terms of dynamic trust, throughput, end-to-end delay, etc. Next, we apply the Bayesian networks model to the trust management in tactical MANETs. Trust of nodes in the network is analyzed by the Bayesian networks model. Then trust management system can filter malicious nodes. We further study how to provide trust management in the Cognitive Radio (CR)-enabled ad hoc networks in order to enhance the security for both spectrum sensing and data transmission. We introduce trust into the cooperative spectrum sensing procedure by weighted consensus-based algorithm. Finally, the security issues in the network function virtualization (NFV) environment are considered. How to establish a trusted relationship in the NFVs and their services is discussed. The spectrum sensing as a service is introduced and trust is applied in the virtual network functions.

With the three methodologies, Bayesian inference, DST and Bayesian network model, in the uncertain reasoning, the trust formulated by them can effectively mitigate the inside attacks in those ad hoc networking paradigms. Extensive simulation results demonstrate that our proposed schemes have better performance than the existing schemes.

Acknowledgments

First of all, I would like to deeply and gratefully thank my supervisor, Prof. F. Richard Yu, for his immense support from all aspects and wonderful supervision. His excellent research insight and intuition and continuous encouragement bring me an amount of momentum to explore the research. His fruitful and talented ideas on the research projects always inspire me in my research. His advice from his plenty of outstanding experience on my research not only help me to complete my PhD research but also direct my future career.

I would like to acknowledge Prof. Long Le, Prof. Jie Liu, Prof. Amiya Nayak, and Prof. Changcheng Huang for serving on my thesis committee.

I would like to thank Dr. Helen Tang, for her valuable comments and suggestions during my research and study. Besides, I want to thank Dr. Jun Li and Dr. Yifeng Zhou for giving me a lot of support and valuable advice in my research.

I would like to thank my colleagues at Carleton University, including Dr. Yegui Cai, Mr. Yanwei Wang, Mr. Zhiyuan Yin, Mr. Chengchao Liang and Dr. Shengrong Bu. I also appreciate the service and support from the staff in our department, who have patience and passion to help every student.

I greatly appreciate my parents and my wife for their understanding throughout the journey of my PhD study.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACK	ACKnowledgement
API	Application Programming Interface
AI	Artificial Intelligence
AODV	Ad hoc On-Demand Distance Vector
ARQ	Automatic Repeat reQuest
AWGN	Addictive White Gaussian Noise
AWS	Amazon Web Services
BI	Bayesian Inference
BNs	Bayesian Networks
CBR	Constant Bit Rate

CPD	Conditional Probability Distribution
CR-MANETs	Cognitive Radio Mobile Ad hoc NETworks
CRNs	Cognitive Radio Networks
CR-VANETs	Cognitive Radio Vehicular Ad hoc NETworks
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DAG	Direct Acyclic Graph
DoS	Denial of Service
DST	Dempster-Shafer Theory
IDS	Intrusion Detection System
IE	Incumbent Emulation
IPv4	Internet Protocol version 4
JSSDT	Joint Spectrum Sensing and Data Transmission
MAC	Media Access Control
MANET	Mobile Ad-Hoc NETwork

MPR	Multi-Point Relay
NB	Northbound
NFV	Network Function Virtualization
OLSR	Optimized Link State Routing
OLSRv2	Optimized Link State Routing version 2
PDR	Packet Delivery Ratio
PU	Primary User
PKI	Public Key Infrastructure
QoS	Quality of Service
RF	Radio Frequency
SDN	Software Defined Networks/Networking
SNR	Signal Noise Ratio
SSDF	Spectrum Sensing Data Falsification
SU	Secondary User
TC	Topology Control

TCP	Transmission Control Protocol
TLV	Type Length Value
TPM	Trust Platform Module
TTL	Time to Live
UDP	User Datagram Protocol
VIM	Virtual Infrastructure Manager
VNF	Virtual Network Function
VPN	Virtual Private Network

List of Symbols

T_{AB}	The total trust value that Node A gives Node B
T_{AB}^{S}	The trust value that Node A gives Node B based on direct observation of Node A
T_{AB}^{N}	The trust value that Node A gives Node B based on indirect observation of Node A
T_{AB}^{D}	The trust value that Node A gives Node B based on data packets
T_{AB}^{C}	The trust value that Node A gives Node B based on control packets
λ	The weight for the trust value based on direct observation
ρ	The weight for the trust value based on data packets
γ	A factor of punishment which is larger than or equal to 1
m	a probability measure in the belief function

Ω	frame of discernment
x_i	the spectrum sensing result of Node i
w_{ij}	a weight for SU i to its neighbor j
A	a matrix
N_i	one-hop neighbor set of Node i
ε	a tolerant deviation
x^*	a final common consensus value

Chapter 1

Introduction

1.1 Motivations

Ad hoc networks have decades development history from military applications to civilian services. The evolution of the ad hoc networks also has an impact on the way of people's life in the future. The application of VANETs is a good example for which is changing people driving environments. Meanwhile, the architecture and operation mechanism of networks also are undergoing a huge development, such as network function virtualization. The advance of service and architecture of ad hoc networking accelerates the rate of applications based on ad hoc networks. Eventually, ad hoc networking applications will merge to the all cyber-applications. People use services but not explicitly notice the specific networks and/or technologies supporting them. As Dr. Mark Weiser, the father of ubiquitous computing, mentioned that "the age of calm technology, when technology recedes into the background of our lives" [3]. The ideal service should hide the type of networks and technologies from the end users. One day, computing service will be the same as the utility. People can use it anytime and anywhere but do not realize it as it is non-existing.

In order to achieve this ambitious goal, security is one of the most significant

research topic with the evolution of computer networks. All kinds of networks, from traditional infrastructure networks to wireless self-organized networks, have a variety of security issues crossing all layers in the network architecture. From 1990s, as the rapid development of the Internet, security issues have become more and more important, which are related to the success of the modern civilization based on the Internet. To tackle these security issues, researchers have done many works in the field of cryptographic techniques, which are considered as prevention-based mechanisms or hard protection systems. Nevertheless, there is always a weak point employed by attackers regardless how prevention systems are powerful so that attackers can break through the wall of protection. Once attackers cross the first protection of networks, the prevention-based mechanisms become powerless. Therefore, the detection-based mechanisms, also known as soft protection systems, are invented as second security protection for networks. Trust-based systems are considered as effective detection-based mechanisms and studied widely in network security recently. There are four primary advantages of trust-based systems, which are listed as follows.

- Firstly, trust-based systems can effectively detect and thwart the inside attackers that sneak the prevention-based mechanisms. These inside attacks always emerge in all kinds of networks and have significant impact on the performance of networks.

- Secondly, trust-based systems are flexible and can be deployed in centralized or distributed networks. Therefore, trust-based systems are very suitable for self-organized networks such as MANETs.

- Thirdly, trust based systems can perform trust assessment locally or globally depended on the specific environments.

- Fourthly, trust-based systems need less computation capability and energy consumption, compared to cryptographic techniques.

Due to these attracting features of trust-based systems, research on this field is prosperous recently. In this dissertation, we focus on the issues related to the trust management in emerging ad hoc networking paradigms. There is a fundamental question in trust-based systems that needs to be answered: how to evaluate trust values accurately based on uncertain information and dynamic environments. This question is addressed in this thesis by uncertain reasoning methodologies.

1.2 Problem Statement

This dissertation focuses on the following ad hoc networking paradigms.

- Mobile ad hoc networks: in particular, we apply trust management with direct and indirect observations to protect MANETs from inside attacks. In this case, nodes in the network communicate with each other in one hop. Source nodes need other nodes to forward the packages to destination nodes, which are in more than one hop distance. Due to characteristics of MANETs, we utilize the Baysian inference and DST to analyze the node behavior.

- Tactical MANETs in military environment: tactical MANETs is the basic infrastructure for the modern battle command system. The risk of attacking is higher in networks than that in the normally civilian networks. We apply Bayesian networks to calculate the trust of each node in the network considering a variety of reasons of packets dropping behavior.

- Cognitive radio enabled ad hoc networks: CR-MANETs and CR-VANETs are two important networks. The amount of applications based on these networks

for civilian services are widespread. Due to the shortage and high cost of spectrum bands, CR is a promising technology to facilitate ad hoc networking. Security of these networks also needs to be considered seriously. We propose a trust management scheme for both spectrum sensing and data transmission.

- Vehicle ad hoc networks with network function virtualization: virtualized network functions can improve the flexibility and scalability of VANETs and, to a certain extent, mitigate security threats in the VANETs. However, NFV has its own different security issues when network functions are running on virtual machines. We present a scheme to reduce security risk in NFV environments with trust.

Challenges: All of above ad hoc networking paradigms have a possibility of facing inside attacks. The core defending mechanism in this dissertation is the trust based detection system. Therefore, the critical research problem is how to assess each node in the networks precisely with dynamic evidence in a distributed manner. Mathematically, trust can be formulated by the subjective probability, also known as Bayesian probability, due to its definition that trust is a subjective belief that an entity should act as expected [4]. It has five primary properties in the context of distributed ad hoc networks. Firstly, trust is subjective. That means different entities (here, nodes in ad hoc networks) have different trust to the same other entity. This is suitable for Bayesian philosophy. Secondly, trust is intransitive, which means it cannot be deduced that node A trusts node C even though node A trusts node B and node B trusts node C. Thirdly, trust is not symmetric. If node A trusts node B, then there is no requirement that node B must trust node A. Fourthly, trust is changeable following time and space. This nature of trust reflects the uncertainty and continuity. The last one is context aware, which can be decided by the role of the entity in the specific circumstance. Based on these properties, we perform the trust

assessment with uncertain reasoning methodologies: Bayesian inference, Dempster-Shafer theory, and Bayesian networks model. This dissertation aims to address the security issues caused by inside attackers with trust management in the above four ad hoc networking scenarios.

1.3 Dissertation Organization and Contributions

Fig. 1.1 demonstrates the structure and relationship of sections in this dissertation. The first two chapters focus on the MANETs with different uncertain reasoning methodologies to evaluate the trust. We utilize the Bayesian inference for the direct observations and DST for the indirect observations. In the tactical MANETs, we present a trust scheme with Bayesian networks for the indirect observations. After that, we study the trust management for both spectrum sensing and data transmission in CR enabled ad hoc networks. We proposed a weighted consensus algorithm for cooperative spectrum sensing. This can effectively thwart the attacks during the spectrum sensing phase. Finally, we address the inside attacks in VANETs with NFV based on trust management. We will present the details of contributions in each chapter.

In Chapter 2, we provide a brief survey of the related works in the ad hoc networking paradigms and security issues studied in this dissertation, the related literature on networking given trust management, and an introduction to the uncertain reasoning used in the thesis.

In Chapter 3, we consider both direct observations and indirect observations for trust evaluation in MANETs. We analyze trust with direct observations in Bayesian inference and calculate trust with indirect observations in DST. Then we combine these trust for a unified trust management to defend the inside attackers. We make the following contributions:

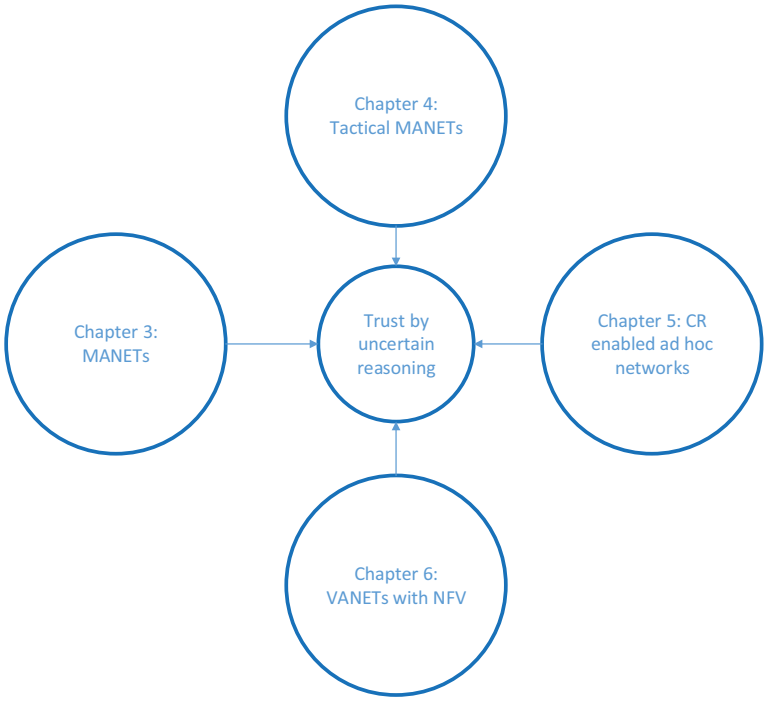

Figure 1.1: The structure and relationship of sections.

- We propose a unified trust management scheme that enhances the security in MANETs using uncertain reasoning. In the proposed scheme, the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method.

- The proposed scheme differentiates data packets and control packets, and meanwhile excludes the other causes that result in dropping packets, such as unreliable wireless connections and buffer overflows.

- We evaluate the proposed scheme in a MANET routing protocol, the optimized link state routing protocol version 2 (OLSRv2) [5, 6], with the Qualnet simulator [7]. Extensive simulation results show the effectiveness of the proposed scheme. Throughput and packet delivery ratio can be improved significantly, with slightly increased average end-to-end delay and overhead of messages.

In Chapter 4, we emphasize on causal reasoning that can facilitate trust evaluation considering the causes of attacks. Additionally, establishment of causal relationships in Bayesian networks can help us make predictions in the presence of interventions [8]. Our scheme uses causal reasoning on the Bayesian networks to evaluate the trust of nodes. The accurate trust value considering malicious intention can be deduced. Chapter 4 contains the following contributions:

- In previous works, researchers use Bayesian networks to combine different dimension trust [9–11], in which a naive Bayesian network model is employed. We propose a normal Bayesian network model with multiple causal relationships between possible reasons.

- Using simulation results, we show that, with the Bayesian networks, trust can be evaluated indirectly and precisely in Tatical MANETs. Therefore, the trust based scheme can mitigate the inside attacks effectively.

In chapter 5, we propose a framework of trust management in CR enabled ad hoc networks. With trust management for both of spectrum sensing and data transmission, the scheme can effectively reduce the chance of inside attacks. This work studies the trust management for cooperative spectrum sensing and data transmission under the dynamic inside attack in the networks. We make the following contributions:

- With the characteristics of CR-MANETs, we identify a new attack, named *joint spectrum sensing and data transmission* (JSSDT) attack, in which an attacker

can report fake sensing data in the spectrum sensing process as well as drop packets in the data transmission process. This attack can extremely disrupt sensing operation and data transmission in CR-MANETs.

- Uncertain reasoning was initially proposed from the artificial intelligence community to solve the problems in expert systems, which have frequent counterfactual results [12]. The elasticity and flexibility of uncertain reasoning make it successful in many fields, such as expert systems, multi-agent systems, and data fusion [12–15]. Using recent advances in the theory of uncertain reasoning [12, 13, 16], we propose a unified trust management scheme for both spectrum sensing and data transmission processes in CR-MANETs. Fig. 5.1 shows the framework of the proposed schemes. Both direct observation and indirect observation are considered in the trust management scheme.

- Based on the unified trust model, we present a weighted consensus-based spectrum sensing scheme to protect the spectrum sensing process. Consensus-based spectrum sensing scheme has been proposed in our previous work [17] to defense against SSDF attacks in CR-MANETs. However, as trust model is not considered in [17], the proposed scheme can be more effective than that in [17]. Simulation results illustrate the effectiveness of the proposed scheme by showing significant improvement in identifying and preventing JSSDT attacks. Both miss detection probability and false alarm probability can be kept below the desired levels.

- We apply the trust value derived from the unified trust model to enhance the security of the data transmission process in CR-MANETs. Simulation results show that throughput and packet delivery ratio can be improved significantly in the proposed routing protocol, with slightly increased average end-to-end delay.

Chapter 6 addresses the security threats in the VANETs with NFV. The challenge is that VANETs with NFV introduce new security holes for inside attackers. Trust management can mitigate the security threats in the NFV environments. We study the trust scheme in the VANETs with NFV. The contributions of this chapter are as follows.

- We propose a joint RSU and vehicle-based light-weighted cloud for CR-VANETs. Based on this cloud computing model, we propose a new service named Spectrum Sensing as a Service (SSaaS), which can perform a cooperative spectrum sensing in CR-VANETs with cloud computing assistance to secure the spectrum sensing procedure. As a result, a reliable service can be obtained in CR-VANETs.
- Simulation results show that the cloud computing and NFV in CR-VANETs can effectively reduce latency and improve the security of CR-VANETs.

1.3.1 List of Publications

The following submitted or accepted papers are partially covered in this dissertation. They are in the order of chapters.

Journal and Conference Papers

Chapter 3: Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning," *IEEE Trans. Veh. Tech.*, vol.63, no.9, 4647-4658, Nov. 2014.

Chapter 3: Z. Wei, H. Tang, F. R. Yu, and P. Mason, "Trust Establishment with Data Fusion for Secure Routing in MANETs," in *Proc. of IEEE ICC'14*, (Sydney, Australia), 2014.

Chapter 3: Z. Wei, F. R. Yu, and A. Boukerche, "Trust Based Security Enhancements for Vehicular Ad hoc Networks," in *Proc. of ACM DIVANet'14*, (Montreal, Canada), Oct. 2014.

Chapter 3: Z. Wei, H. Tang, F. R. Yu, and M. Wang, "Security enhancement for mobile ad hoc networks routing with OLSRv2," in *Proc. of IEEE SPIE'13*, (San Diego, USA), June 2013.

Chapter 4: Z. Wei, H. Tang, F. R. Yu, and P. Mason, "Trust Establishment Based on Bayesian Networks for Threat Mitigation in Mobile Ad Hoc Networks," in *Proc. of IEEE Milcom'14*, (Baltimore, MD, USA), 2014.

Chapter 5: Z. Wei, F. R. Yu, H. Tang, and P. Mason, "A Unified Trust Management Scheme for Both Spectrum Sensing and Data Transmission in Mobile Ad Hoc Networks (MANETs) with Cognitive Radios," to be submitted to *IEEE Trans. Veh. Tech.*.

Chapter 5: Z. Wei, H. Tang and F. R. Yu, "A trust based framework for both spectrum sensing and data transmission in CR-MANETs," in *Proc. of IEEE ICC'15 Workshops*,(London, UK), 2015.

Chapter 5: Z. Wei, F. R. Yu and A. Boukerche, "Cooperative Spectrum Sensing with Trust Assistance for Cognitive Radio Vehicular Ad hoc Networks," in *Proc. of ACM DIVANet'15*,(Cancun, Mexico), 2015.

Chapter 6: Z. Wei, F. R. Yu, H. Tang, C. Liang and Q. Yan, "Securing Cognitive Radio Vehicular Ad hoc Networks with Trusted Lightweight Cloud Computing," in *Proc. of IEEE CRESS'16*, (Philadelphia, PA, USA),2016.

Chapter 2

Related Work

This chapter provides a review of the literature related to this dissertation.

2.1 Ad hoc Networking Paradigms

In this section, we introduce the four types of ad hoc networking paradigms, which are used to study the trust management for mitigating security issues.

2.1.1 Mobile Ad hoc Networks

Mobile ad hoc networks are originated from military environments. The initial purpose of the design is that military tactical network can work in the harsh battlefield to guarantee communications between battle units and improve the solders' survivability [18]. In the modern war environment, traditional communication infrastructure is always the target that enemies attack with a high priority. MANETs can provide temporary communication networks so that military communications, such commands from headquarters, can avoid destruction and pass to the battle units. This special capability of MANETs also can apply to non-military environments. As the price of basic networking device declines, MANETs gradually are applied into the

civil and commercial areas. Then the application of MANETs extends to emergency environments, e.g., temporary communication networks after earthquake, which can help different groups to disseminate information and organize activities. Compared to traditional networks, MANETs have no centralized server to manage the whole network. Without pre-defined infrastructure, each entity, a.k.a node, has to depend on other nodes to transfer the data. That means nodes not only generate information and receive information, in which they are interested, but also need to cooperate to forward the traffic for each other in MANETs.

Due to the lack of pre-defined infrastructure, mobile node has to be aware of other nodes within its radio range. These nodes in the radio range are called one-hop neighbors. If the nodes are neighbors, they can communicate both directions with the wireless link. Only nodes, which are directly connected or connected by other nodes can send and receive data from each other. This type of self-organized network can form different topology due to the nomadic nature of nodes from time to time. When data are sent from a source to a destination, each node in the path, except the source and destination node, should forward the data packets.

The distinguishing features of MANETs are listed below [19].

- The network is comprised of independent nodes autonomously. Nodes can join in and leave the network at freedom. This leads to the dynamic changing of the network topology.

- Communication between nodes needs cooperation of other nodes. Nodes only can transfer and receive data from its one-hop neighbors. Thus multi-hop routing is the essential scheme for MANETs, which can coordinate node in a distributed manner to forward packets in the entire network. Self origination and cooperation are the key to success in MANETs.

- Due to the self organization nature and limited resource of each node, the energy

consumption is a big concern of each node. Thus energy efficiency mechanisms decide the life span of MANETs.

- The configuration and deployment of the network are cheap and simple. Therefore the scalability of MANETs is better than traditional networks. MANETs are suitable from a small scale to a large scale.

Routing in MANETs is a hot research topic. Several routing protocols for MANETs are standardized by IEEE, such as OLSR (v1 and v2) [5, 6], DSR [20], AODV [21] etc. Here we describe the OLSRv2 in more details, which is applied to our scheme in Chapter 3. OLSRv2 is a proactive routing protocol, which is a new version of OLSR [5]. OLSRv2 inherits OLSR's core algorithms and also introduces some new features [6]: routing Multipoint Relay (MPR), flexible link metrics, extensible message formats, etc. OLSRv2 has three basic components: Neighborhood Discovery, MPR Selection, and Topology Establishment, as well as two types of control messages: a HELLO message and Topology Control message [6]. Neighborhood Discovery [22] is used to facilitate a node's discovery of its one-hop neighbors in radio range. HELLO messages, which can carry link status such as symmetric, asymmetric, or multipoint relay, are used in the neighborhood discovery procedure. Through periodically sending HELLO messages, a node can establish bi-directional (symmetric) links with its one-hop neighbors. Two types of MPR selection: flooding MPR selection and routing MPR selection, are performed in OLSRv2. Flooding MPR selection plays a key role in forwarding control traffic in the network. A node selected by a neighbor of this node as a flooding MPR will forward the message from the neighbor once. This mechanism can effectively reduce the total transmission in the network. Routing MPR selection is separated from flooding MPR selection in OLSRv2. The main function of routing MPRs is to disseminate link state information by TC messages. This mechanism can reduce the size of link statement information that is sent

in order to limit the network topology. A network topology is established by link state information diffusion. Routing MPRs connect multi-hop routes in the network.

Although OLSRv2 provides extensions for customization, there is no specific security mechanism in the protocol. Consequently, OLSRv2 is susceptible to various attacks such as worm hole attacks, black hole attacks, spoofing, jamming, and so on [23, 24].

In this thesis, one trust scheme is proposed as a security mechanism that mainly protects OLSRv2 against two types of misbehavior, dropping packets and modifying packets. Packet dropping attack is also called as a black hole attack, which is a type of denial-of-service attacks [25]. Modification of packets may have a significant impact on a topology map [26].

2.1.2 Vehicular Ad hoc Networks

VANETs, usually, are regarded as a particular type of MANETs in the literature [27]. In VANETs, there are primary characteristics, which are different from traditional ad hoc networks. Firstly, VANETs are a specific purpose system for vehicles in order to provide a safe and efficient transportation environment. MANETs are more general than VANETs, which can be deployed in many different environments for multiple purposes. Secondly, VANETs have a strong regulation in the mobility and types of nodes. Due to the road planning of cities and states, the speed and direction of a vehicle are strict. MANETs are more flexible than VANETs. Thirdly, messages in VANETs have a high sensitivity of location and time, for examples, weather warnings and congestion information. In the two basic communication ways of VANETs, V2I is more reliable and permanent because road-side infrastructure units (RSUs), which are constructed by transportation departments, have more energy and computing capability for security, for examples, complicated cryptographic algorithms, fire walls,

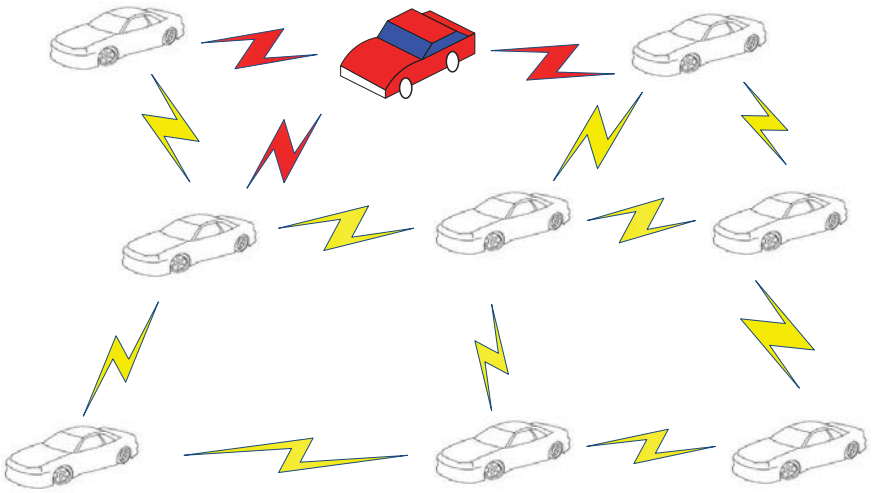

Figure 2.1: A typical VANET with a malicious vehicle.

strong access control systems etc. In V2V, vehicles send messages with each other without centralized infrastructure and relay information for other vehicles. Each vehicle can perform as an autonomous entity with full capability. In this way, each vehicle needs to judge if the message or the other vehicle is trustworthy.

Fig. 2.1 depicts a typical VANET, which comprises normal vehicles and a malicious attacker. The attacker will disrupt the normal performance of the VANET. The detail of attacks employed in VANETs will be described in the security issues section later.

2.1.3 Cognitive Radio Enabled Ad hoc Networks

Cognitive radio as a promising technology is proposed to solve the scarcity of spectrum resource. CR is originated by Dr. Joseph Mitola III in his dissertation [28]. This new technology can utilize the idle spectrum bands, which are licensed to other users. Because CR has an ability to dynamically adjust the its parameters based on radio traffic requirements in order to suit for the current environments, including time and

space changing. Due to the advances of software defined radio, the parameters of radio are configured feasibly and easily. CR not only extremely extends the limited spectrum resource lifespan, but also improves the efficiency of spectrum utilization.

The primary idea of CR is that the entity with CR can access the licensed spectrum bands, which are owned by the paying user, also known as the primary user (PU). The pre-requisite is that the CR user, which is unlicensed, should not interfere the PU's communication. In other words, the unlicensed user, also known as secondary user (SU), has the ability to detect the presence of the PU and then gives back the right to the PU that own the licensed spectrum. The well-known licensed spectrum bands, which can be used by SUs, are TV resource, also known as TV white spaces (TVWSs). TVWSs are a type of time-based temporary under-loaded spectrum. As the diversity of entertainments with the new technology such as Internet, TVWSs have been becoming a bonanza of the spectrum resource. Standard organizations have proposed standards for TVWSs, e.g. IEEE 802.19, which can leverage the CR technology to a large extent.

There are three kinds of mechanisms to identify the primary users that is present during the spectrum sensing [17].

- Energy detection: this method is easy to be implemented, but it is a suboptimal method. There are fewer requirements for the position of PUs than other methods.

- Matched filter: this method is much more complex than others, but it is an optimal method; it needs to develop different types of adaptive sensing circuits based on the different primary wireless systems.

- Cyclostationary feature detection: this method can detect the signals with a very low SNR. However, it requires some prior knowledge of PUs.

2.1.4 Cloud Computing and NFV in VANETs

Cloud computing can primarily improve the availability of computing from individuals to large companies with dynamic scalability. It makes the computing utilization as using electricity easily and conveniently [3]. Cloud computing is treated as a public utility, which can provide services following different fast-changing requirements. Before explanation of cloud computing, what is cloud needs to be introduced firstly. Cloud is defined as the data centre that is comprised of hardware and software systems running on the hardware [29]. Cloud computing includes the data centre and the applications provided by the data centre. The applications can be sold by the data centre owner as services. There are three types of well-known services in the cloud computing area [29]. Software as a Service (SaaS) can provide specific applications for end users. For example, Dropbox [30] provides storage services for users. Users can order different amount of storage spaces with different prices. GitHub [31] provides the service for version control of code. Individual developers, open source communities, or big companies purchase this service for their software projects management. Platform as a Service (PaaS) can allow end users to run their applications in the cloud service. Google App Engine [32] is a kind of this service, which provides an operating environment to run costumers' Java or Python or PHP programmes. Infrastructure as a Service (IaaS) can provide all basic resources for end users. Users can own their specific operating system in the cloud service. Windows Azure [33] is this kind of services, which can install different operating systems with different customers' requirements. All the three types of cloud services rely on an importantly elementary technology, which is virtualization. It is originated from the computer science community in 1970s [34]. Although this concept is not new, it provides a cornerstone for the cloud computing. All kinds of cloud services utilize the virtual machines to provision the functions under the requirements from clients. Each virtual machine

has its own computing resource such as CPU, storage space such as memory and hard driver, and IO capability. Hypervisor that underlies virtual machines is in charge of the real hardware resources scheduling. This ability can improve the scalability of cloud services. End users don't notice the changing of hardware resource. This makes the resource allocation according to the current and real needs possible. Therefore, "pay as you go" is the elementary profit model for cloud computing providers [29].

As the one type of widespread application of cloud computing, network function virtualization have been becoming imperative for giant telecommunication corporations. Because NFV can help data centres to abstract the network management and configuration flexibly and easily. NFV is different from the traditional VPN [35], which only splits the physical local network to small pieces that hidden the internal configuration and operations from each other. NFV can decouple the network functions from physical network hardware totally. The underlying network devices become the dummy forwarding machines that have no idea about the real business of the network, such as routing, security configuration, QoS etc. Fig. 2.2 shows that the traditional networking devices in the left rectangles are physical appliances with embedded software for the fixed and single purpose. The traditional networking solution is hard to be configured and extended. When new customer requirements come in, it almost hardly evolves to provision new services in a short time period. After traditional solutions evolve to NFV solutions, network service providers can implement the network deployment and updating seamlessly due to the scalability and agility of NFV.

NFV as a stunning technology will entirely change the network industry. Because it enables telecommunication companies as primary operators of network services to satisfy the new and dynamic changing requirements from their customers. More important, the network services based on NFV can evolve with the requirement with the

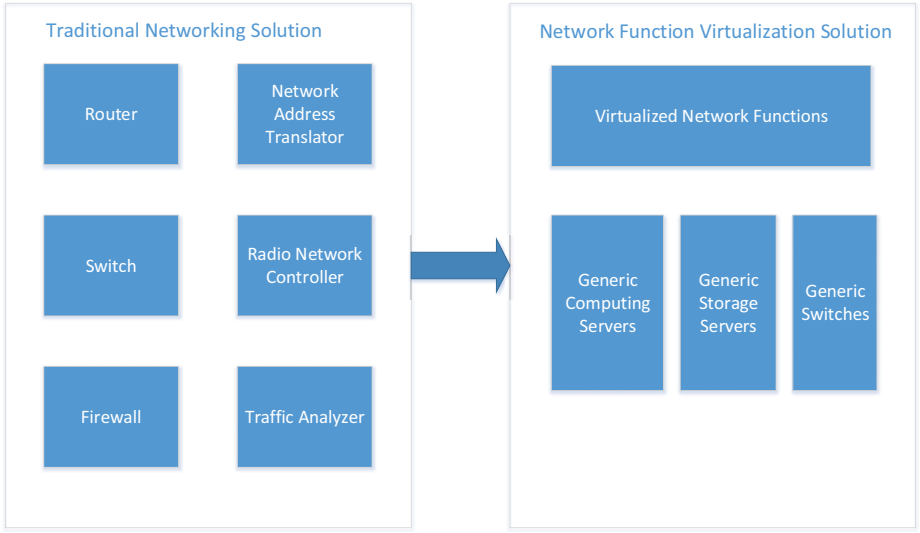

Figure 2.2: Transferring from traditional network devices to NFV [1].

lower cost than before. In other words, NFV makes the network service highly customized and agile as software. NFV enhances the scalability of the network services, which can embrace the innovative business models feasibly.

NFV moves the basic network functionality, which formerly is embedded in the network devices to the high level software through the network hypervisor [1] that is similar to the hypervisor in the virtual machine. Virtualization of networks opens a new view of the entire network infrastructure. It abstracts the physical functions into virtual resources [1]. Virtualizing the basic physical network is a process to abstract, slice, isolate, and share the entire physical networks. Fig. 2.3 shows the architecture framework of NFV. From top to down, the network service is a module that provides the business values for the customers. All requirements are implemented in this module. Network service needs NFV management and orchestration to define and translate to the lower layer, VNFs. VNFs stand for different specific network functions, like routing and fire wall. Each VNF is deployed and managed by a VNF life-cycle manager. In the VNF life-cycle manager, each VNF has its own resource, which is allocated during the deployment. The VNF life-cycle manager also monitors

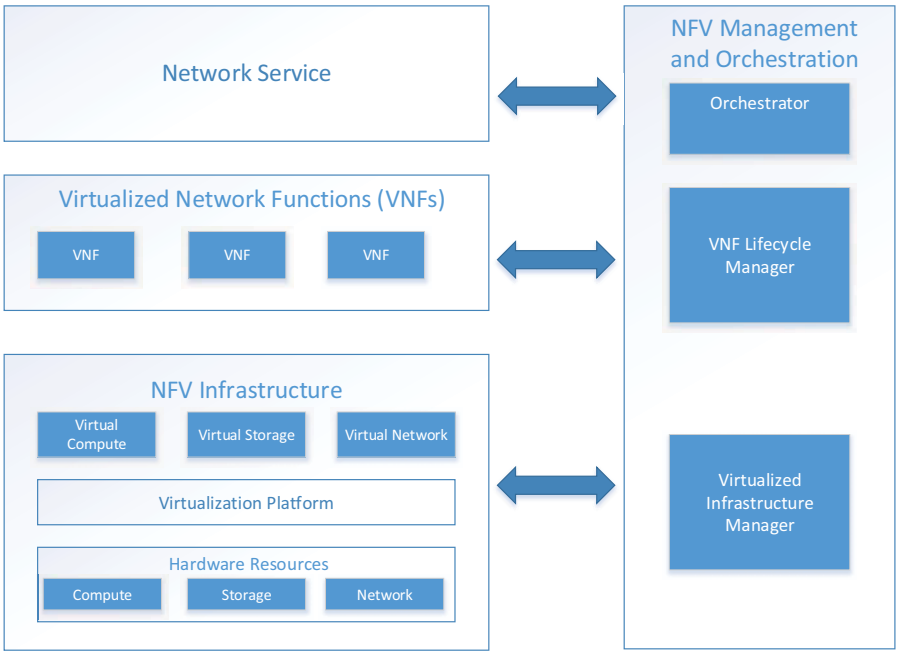

Figure 2.3: The architecture framework of NFV [2].

all VNFs. Based on the different situations, the VNF life-cycle manager can perform recovery and scaling out/in actions for the VNF. NFV management and orchestration utilizes the VNF life-cycle manager to achieve the business logic. VNFs are laying on the NFV infrastructure module, which provision the virtual resources such as computing, storage, and networking. In the NFV infrastructure, the virtualization platform plays a key role, which can transform the hardware resources to the virtual resources. It is also known as the hypervisor layer. OpenStack [36], VMware vCentre [37], and AWS [38] belong to this platform. Virtualized infrastructure manager is a software component that controls all the NFV infrastructure. It abstracts the key functions of low level virtual resources and presents the standard APIs for the VNF life cycle manager. From high level applications, there is no need to know details of NFV infrastructure. The virtualized infrastructure manager provides the flexibility for the users to dynamically and seamlessly change the NFV infrastructure, e.g., from OpenStack to vCentre.

Several cloud computing models in VANETs are proposed. In [39], the authors propose a cloud computing model for VANETs, named VANET-Cloud, which extends the cloud to the vehicles. In this model, there are two types: permanent and temporary. A vehicular cloud networking model is proposed in [40], which combines the vehicular cloud computing and information-centric networking. This model can provide efficient services for drivers. The authors in [41] present a vehicular social network in cloud computing, which can help the useful information transmission for users who are interested in. In [42], a three-layer cloud computing model in VANETs is presented. In this cloud-based vehicular network, the resource management is studied with a game-theoretical mechanism. Resource management for cognitive cloud vehicular networks is studied in [43]. The authors use an optimization scheme to solve this resource management problem. Fog computing paradigm in VANETs is studied in [44]. Due to the requirement of dynamic, local, and delay-limited nature of VANETs, fog computing can become a useful alternative of conventional cloud computing. In [45], the authors propose vehicular node virtualization, which allows the service provider to allocate resources to tenants within vehicular nodes. The virtual machine migration in VANETs is also studied.

2.2 Security in Ad hoc Networking Paradigms

In this section, we explain the different security concerns in the ad hoc networking paradigms.

2.2.1 Security Issues in MANETs and VANETs

Due to the distributed and dynamic nature of MANETs, they have more vulnerabilities than traditional pre-defined infrastructure networks. No centralized authority

and unstable wireless connection between nodes may introduce more challenging security issues in the network design. Node-based security mechanisms are the main protection means for MANETs. Traditional centralized network security solutions are hardly applied to MANETs.

The basic security mechanisms in MANETs are as follows [19].

- Data integrity is used to prevent the tampering forward information between nodes in the network.
- Confidentiality can protect the communication data from eavesdropping attacks.
- Access control can thwart the attacker obtaining information from wireless connections.
- Intrusion detection can exclude the attacker that joined in the network.

Major security threats in MANETs include denial of service(DoS) attacks, blackhole attacks, wormhole attacks, host impersonation, resource consumption attacks, passive eavesdropping, information stealing, and physical radio/signal interference [19]. Security issues in MANETs have been studied comprehensively. Basically, there are two complementary categories of mechanisms to safeguard MANETs: prevention-based solutions, which mainly focus on cryptographic techniques and systems in order to thwart the attackers from the outside of the network [46]; detection-based solutions, which focus on the detection of inside attackers that have already knocked the first protection down [46]. Intrusion detection systems serve as the second wall of protection, which can effectively identify malicious behavior of the inside attackers.

VANETs have distinguishing features based on the requirement of driving safety, traffic efficiency and traveling entertainment. Although VANETs always are considered as a specific case of ad-hoc networks, they have different environment and application scenarios. Therefore, attacks in VANETs focus on diverse aspects from

application to physical sensing, from Vehicle-to-Vehicle to Vehicle-to-Infrastructure. The security requirements in VANETs include privacy, integrity, and confidentiality. For example, if the emergency information is fake or modified by the attacker, the whole traffic may be influenced simultaneously. Meanwhile, the privacy of drivers and passengers also needs to be protected. When the emergency message is received by a malicious vehicle, it adds some spiteful delays to the original message instead of forwarding it to the neighboring vehicles at the right time. Therefore, the timing issue can cause the incorrect information for the target service in order to mislead the end users. Although the new attacks in VANETs extremely threaten the driving safety, the traditional attacks in MANET environments still need to be solved properly, such as Sybil attack and DoS [19].

2.2.2 Security Issues in CR Enabled Ad hoc Networks

In CR-MANETs, each node performs routing and transmission actions autonomously through wireless links. CR-enabled nodes have the capability to detected the unused spectrum and then select the suitable channels for data transmission. However, except traditional attacks in MANETs, CR-MANETs are facing more security challenges due to spectrum sensing features. Traditional security issues in MANETs include denial of service, black-hole, resource consumption, information disclosure, and interference. For the new attacks in CR enabled environments, researchers have done some excellent works. In [47], researchers presented two types of attacks performed by outside attackers: jamming attacks and incumbent emulation attacks. In a jamming attack, the attacker pro-actively generate a large amount of noise to pollute the sensed channel. This behavior will interfere the normal sensing procedures performed by normal node in the network. The target of the radio jamming attacks is to interfere the

communications in the physical layer and the link layer of the networks [47]. Generally, two types of jamming attacks are presented in the literature. The first one can occupy the wireless licensed spectrum all the time, therefore the legitimate users have no chance to access the open spectrum. The other one can corrode the SNR by disseminate data around the neighbors of the target victim. The authors from [47] presented a security threat, in which the outside attacker can generate and send jamming signals to sensors, control channels or even any destination node in order to disrupt the normal Cognitive Radio Networks (CRNs) service. The interference-resilient communications schemes are proposed, which can decipher the transmission signals from others using very low SNR regimes.

Some works also have been done in the research of SSDF attacks under the centralized network model with SUs [48–52]. In [48], the researchers propose a scheme, named Weighted Sequential Probability Ratio Test, which can effectively protect spectrum sensing operation from SSDF attacks. In [49], the authors present a framework to collect spectrum sensing data from diverse sources in a grid of square cells. Through the outlier identification mechanism, malicious nodes in the interested area can be detected. In [50], an abnormality detection approach is proposed, which can exclude malicious nodes without prior knowledge about attack strategies. The authors of [51] propose outlier detection techniques without complete information of PU and plenty of sensing data samples to identify malicious SUs. In [52], the authors describe an onion-peeling approach based on Bayesian methodology, which can find and exclude malicious nodes when suspicious levels are beyond a threshold.

In addition to this SSDF attack introduced in CR environments, traditional attacks, e.g., packet dropping attack and packet modification attack, can still affect CR-MANETs. Since one of the most important security objectives is to protect data

transmissions between sources and destinations, many researchers devote their enthusiasms to this research field [23, 26, 53–60]. These security mechanisms can be classified to two basic categories: prevention schemes and detection schemes [46]. In prevention schemes, a variety of cryptographic techniques can be applied to thwart attackers to obtain the original information [23, 26, 53, 54]. In detection schemes, researchers utilize intrusion detection systems and trust management to identify and exclude malicious intruders [55–60].

In decentralized CR networks with mobile SUs, it is necessary to protect distributed cooperative spectrum sensing mechanisms [61]. The authors of [62] present a new attack model, named covert adaptive data injection attack, which targets at the distributed consensus-based spectrum sensing scheme. In this attack model, malicious SUs can dynamically change the reported values of an incumbent energy in order to avoid the fixed threshold detection during the distributed consensus-based spectrum sensing procedure.

Security issues of spectrum sensing in CR are studied extensively, and several mitigation schemes are proposed in the literature [48, 51, 52]. A Bayesian methodology is used in [52] to detect and filter out the malicious nodes with a threshold. The researchers in [48] present a Weighted Sequential Probability Ratio Test to protect spectrum sensing from SSDF attacks. The authors of [51] utilize outlier detection techniques to identify malicious SUs. The techniques don't require full information of PU and the amount of sensing data samples is less than in other schemes. A distributed cooperative spectrum sensing mechanism is studied in [61]. The authors describe a consensus-based algorithm to detect the status of PU. A variant SSDF attack, named covert adaptive data injection attack is proposed in [62], which can attack the node during the distributed consensus-based spectrum sensing.

2.2.3 Security Issues in Cloud Computing and NFV for VANETs

Based on the description of subsection 2.1.4, cloud computing and NFV both are established on the virtual machines. Hypervisors schedule the physical resources for virtual machines in order to implement the network services. Security policies or rules are easier to be deployed in the virtual networks. It enables the flexibility and agility of security service upgrading when attacks happened in the network. To some extension, NFV can leverage the security level of the network service through the dynamic and different security rules deployment. However, the security threats are still existing in the NFV area. Generally, there are three categories of security issues [42]. First one is security concerns in the virtual machines. For example, the security holes may exist in the network virtualization environments due to the sharing physical resources among virtual machines for different services. Even if accidental abusing resource happens, the service that depends on virtual machine can be affected importantly and finally fail to provide functions to the end users [63]. This type of security attack also can cause memory leakage, software malfunction, isolation disorder etc. Second one is traditional network attacks, such as DoS, eavesdropping, black hole attack, and Sybil attack. The third one is the joint virtualization and networking attack, which can utilize both aspects in the NFV. Software security holes or malfunction attacks may be worse than traditional network services based on the function embedded physical networking devices. Attackers explore the software vulnerability in the virtual machines and then gain the higher access control right. Due to the virtualized network functions based on virtual machines, attacker can further control the networking functions, such virtual routing. Therefore, attackers can easily paralyze any network service that is established on the VNFs. Topology attack is another threat in the NFV environment [1, 63]. Normally, NFV is composed by

amounts of VNFs, which can form arbitrary service chains. Attackers can exploit the service chains to generate loops in the chains. This malicious behavior can extremely interfere the traffic, even if simple loops occur in the chains. Another security threat in NFV is how to manage the network infrastructure when the underlay networks is attacked or malfunction. Although this issue is existing in the traditional networks, it may be worse in the NFV due to the physical resource sharing. Backup networking resources sometimes are expensive for the small company clients. NFV needs more accessing capabilities when VNFs start working. Initial configuration needs network connectivity, which may rely on another VNF. This is a looping problem if the relied VNF is attacked. Secure boot issue [1] also roots in the NFV due to the hypervisor application. Trusted platform module is a general and standard solution for this issue not only in the NFV environments but also in all operating systems. Virtualization crash is an important security issue due to the first class position of software in NFV. Two types crashes affect the NFV. Applications running in the virtual machine crash somehow. It is isolated properly by hypervisors. It should not impact on other applications in the virtual machine. Virtual machines crash, which implement the specific VNF. This kind of crash need to be tackled carefully. Because many resources are related to the VM, which can be utilized by attackers, such as spoofing or masquerading. NFV may introduce more challenging security issues for tenant authentication, authorization and accounting. This is because that the NFV framework is made of three-level functional modules with more flexibility and scalability. Different modules need authentication and authorization when they cooperate and collaborate, especially in multiple-tenant use cases.

2.3 Trust-based Methodology for Security

Trust is studied by sociology at first and attracts researchers' attention from different disciplines including psychology, economy, management science, security etc. [4] Trust defined by sociology is explained as the degree of belief that an agent performs specific jobs [4, 64]. Trust is an abstract concept, which is related to different concepts, such as reputation, confidence, recommendation, risk, belief, and so on [65]. Trust definition is described that under the specific context, trust is the subjective opinion and assertion from an agent to another agent through the observation [65]. It also presents the expectation of the observed agent's future behavior. Trust usually is associated with risk. In [66], trust is depicted as a predictor that concrete behavior is performed in the future. The more trusted agent fails to act as expectation, the higher risk will be resulted to. Trust can also be defined as a relationship in a community, especially social networks [67]. In order to utilize trust effectively in the practical systems, trust management is proposed [68]. Trust management is a unified methodology to define, regulate, and interpret security related policies, credentials, and relationships in the systems [68]. Trust management is a composite of different components: trust establishment, trust computation, trust aggregation, trust propagation, trust update, and trust revocation [4, 65].

Trust-based security schemes are important detection-based methods in MANETs, which have been studied recently [4, 13–15, 46, 57, 58, 69–77]. In [57, 69], the trust value of a node based on direct observation is derived using Bayesian methodology. The authors of [58] regard trust as uncertainty that the observed node performs a task correctly, and entropy is used to formulate a trust model and evaluate trust values by direct observation. Compared to direct observation in trust evaluation, indirect observation or second-hand information can be important to assess the trust of observed nodes. For example, the collection of testimonies from neighbor nodes

can detect the situation where a hostile node performs well to one observer, while performing poorly according to another node.

Trust based security systems are also studied in different network architectures, e.g., wireless sensor networks [59, 78], vehicular ad hoc networks (VANETs) [79], cooperative wireless networks [80], etc. Although different types of networks have different specific characteristics, the proposed trust model based on direct and indirect observation is general enough and can be customized to a particular network. Marti *et al.* [55] propose a trust-based scheme including watchdog and pathrater to secure the dynamic source routing algorithm in MANETs. Sun *et al.* [58] develop a framework to model and evaluate trust in ad hoc networks, where entropy is used to measure trust. Considering the importance of second-hand information for trust assessment, some researchers use both first-hand and second-hand information to trust evaluation. Buchegger *et al.* [56] propose a distributed reputation system for MANETs based on the Bayesian approach. Second-hand information is used for trust rating in the system. Zouridaki *et al.* [57] combine first-hand trust information with second-hand trust information in order to improve the reliability of data transmission. Trust-based routing solutions are also studied in wireless sensor networks. In [59], a trust-aware dynamic routing framework is proposed. Self-observations (first-hand information) and recommendation (second-hand information) are used in this framework to evaluate trust. In CR environments, a trust-based collaborative spectrum sensing scheme is presented in [81], in which authors utilize Location Reliability and Malicious Intention as two trust measurements to fuse spectrum sensing data and make decisions in the centralize infrastructure.

The security mechanisms for routing protocols in MANETs have been studied comprehensively. There are two basic approaches of protection for routing protocols:

prevention-based solutions and detection-based solutions. The prevention-based solutions [23, 54] can thwart the attacks from outside of the network. However, these cryptographic techniques usually make the network suffer extraordinary overhead due to the key sharing and verification between nodes [82]. Because of dynamic natures of MANETs and the increasing number of inside attacks, trust-based intrusion detection approaches are drawing a lot of attention from researchers.

Marti *et al.* [55] propose a trust-based scheme that secures the dynamic source routing algorithm in MANETs. This scheme consists of two components: watchdog and pathrater. The watchdog component detects misbehaving nodes and the pathrater component assesses the reliability of nodes and makes decisions. Sun *et al.* [58] develop a framework to model and evaluate trust in ad hoc networks. In this framework, entropy is used to measure trust. Considering the importance of second-hand information for trust assessment, some researchers use both first-hand and second-hand information to trust evaluation. Buchegger *et al.* [56] propose a distributed reputation system for MANETs based on the Bayesian approach. Second-hand information is used for trust rating in the system. Zouridaki *et al.* [57] combine first-hand trust information with second-hand trust information in order to improve the reliability of data transmission. Trust-based routing solutions are also studied in wireless sensor networks. In [59], a trust-aware dynamic routing framework is proposed. Self-observations (first-hand information) and recommendation (second-hand information) are used in this framework to evaluate trust. In [76], authors propose a new trust computation and management system, in which the community concept is applied. In [73, 75], authors present an agent-based trust and reputation management scheme in wireless sensor networks, considering the overhead of the message passing and time delay. In [74], authors propose a trust based system to protect the ubiquitous and pervasive computing environments, in which a trust model is developed

and based on the trust, the access control can be made and the private keys are updated. In [77], authors present a trust based multi-cast scheme for the mobile health system. In the scheme, a new trust assessment model is developed. A secure multicast scheme utilizes trust of each node and allows the trusted node to participate the communication in the system.

2.4 Uncertain Reasoning

In this section, we present three methodologies in uncertain reasoning: Bayesian inference, DST, and Bayesian networks model.

2.4.1 Bayesian Inference

Bayesian philosophy is very suitable for the explanation of trust in mathematics. Due to the definition of trust in the Section 2.3, we need a tool to formalize the trust and trust computing. The goal of Bayesian inference is to calculate and analyze the subjective degrees of belief [83]. Therefore, Bayesian inference is applied to evaluate trust in our research problem context. Bayesian inference is a procedure of obtaining knowledge of an unknown target variable from existing data or simple assumption of data [84]. From the Bayesian point of view, trust is considered as a random variable with a known distribution, in our context, which is Beta distribution. Bayesian inference tries to calculate the random variable, which is described by a model from the realm of probability theory. Based on the observed events, Bayesian theorem is applied to continuously improve the target variable, known as a posterior probability distribution. In order to complete the process of Bayesian Inference, there are three basic steps as follows. Firstly, the prior probability need to be known and the conditional probability distribution should be known either. Then, observation of evidence

is performed. Based on the observation, the Bayes' rule is applied to calculate the posterior probability distribution. Finally, the estimation can be made by different methods, such as least mean squares estimation [84].

2.4.2 Dempster Shafer Theory

The Dempster-Shafer theory (DST) is regarded as a useful mechanism in uncertain reasoning and is widely used in expert systems and multi-agent systems [13, 14]. In [15], the Dempster-Shafer theory is used in sensor fusion. Intrusion detection systems [46, 70] apply the Dempster-Shafer theory to assess unreliable information from IDS sensors. In [71, 72], the Dempster-Shafer theory is used to detect the malicious nodes and isolate them in ad hoc networks.

We use uncertain reasoning theory from artificial intelligence to evaluate the trust of nodes in MANETs. Uncertainty is an old problem from gambler's world. This problem can be handled by probability theory. Reasoning is another important behavior in everyday life. A lot of researchers, even Aristotle (384 BCE - 322 BCE) (Greek Philosopher), try to understand and formulate it. Reasoning based on uncertainty has been prosperous in the artificial intelligence community due to the development of probability theory and symbolic logic. Probabilistic reasoning is introduced to intelligence systems [12], which is used to tackle the exceptions in automatic reasoning. In order to overcome the drawbacks of traditional rule-based systems, which are based on truth tables with no exceptions, probabilistic reasoning is proposed, in which the uncertainty of knowledge is considered and described as subsets of "possible worlds." Probabilistic reasoning can be used to different areas, from artificial intelligence to philosophy, cognitive psychology, and management science. In the area of security in MANETs, we find that this theory is very suitable for trust evaluation based on the trust interpretation in this thesis. Bayesian inference and Dempster-Shafer evidence

theory are two approaches in uncertain reasoning. We adopt them to evaluate trust of nodes by direct and indirect observation.

2.4.3 Bayesian Networks Model

Based on the special characteristics of Bayesian networks, many research works tried to use this tool to evaluate trust in distributed networks [9–11, 85–87]. A naive Bayesian network based trust model is proposed in peer-to-peer networks by [11]. Authors utilize the Bayesian network model to evaluate trust based on different service properties. Another Bayesian network based trust model is used in MANETs [10]. Authors of this paper combine direct trust and indirect trust in the proposed trust model. Although maliciousness detection is mentioned in this paper, the trust model still only considers provided service, which is similar to [11]. Authors in [9] proposed a trust model based on Bayesian networks in wireless sensor networks. Trust in this model is comprised of communication trust and data trust, which are combined using a Bayesian network. However, authors in [9] do not demonstrate how to analyze each trust component by the Bayesian network. In [85], authors apply a naive Bayesian filter, a simple type of Bayesian networks, to classify nodes in MANETs. This approach establishes early node profiles without extra recommendation exchange. Authors in [86] present an approach to evaluate trust based on a modified Bayesian based confidence model. This approach provides reliable routing paths between source nodes and sink nodes based on trust. Authors in [87] propose a trust approach based on Bayesian Networks for QoS in web service applications. A multinomial generalized Dirichlet distribution is used in learning Bayesian networks to model QoS.

Chapter 3

Trust Management in MANETs

3.1 Introduction

With recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks (MANETs) [88] have become popular as a key communication technology in military tactical environments such as establishment of communication networks used to coordinate military deployment among the soldiers, vehicles, and operational command centers [19]. There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium, nomadic and distributed nature, lack of centralized infrastructure of security protection [23, 26, 55]. Therefore, security in tactical MANETs is a challenging research topic [89].

There are two complementary classes of approaches that can safeguard tactical MANETs: *prevention-based* and *detection-based* approaches [46]. Prevention-based approaches are studied comprehensively in MANETs [23, 26, 53, 90, 91]. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields.

If the infrastructure is destroyed, then the whole network may be paralyzed [55]. Furthermore, although prevention-based approaches can prevent misbehavior, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing establishment. From the experience in the design of security in wired networks, multi-level security mechanisms are needed. In MANETs, this is especially true given the low physical security of mobile devices [92, 93]. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities [94, 95].

Although some excellent work has been done on detection-based approaches based on trust in MANETs, most of existing approaches do not exploit direct and indirect observation (also called secondhand information that is obtained from third party nodes) at the same time to evaluate the trust of an observed node. Moreover, indirect observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node [56, 57, 69]. Therefore, inaccurate trust values may be derived. In addition, most methods of trust evaluation from direct observation [57, 58, 69] do not differentiate data packets and control packets. However, in MANETs, control packets usually are more important than data packets.

In this chapter, we interpret trust as the degree of belief that a node performs as expected. We also recognize uncertainty in trust evaluation. Based on this interpretation, we propose a trust management scheme to enhance the security of MANETs. The difference between our scheme and existing schemes is that we use uncertain reasoning to derive trust values. Uncertain reasoning was initially proposed from the artificial intelligence community to solve the problems in expert systems, which have frequent counter-factual results [12]. The elasticity and flexibility of uncertain reasoning make it successful in many fields, such as expert systems, multi-agent systems, and data fusion [12–15].

The remainder of this chapter is organized as follows. The trust model and its two components are presented in Section 3.2. Section 3.3 depicts the Bayesian methodology and how to use it in trust evaluation from direct observation. Section 3.4 describes the Dempster-Shafer theory and how to use it in trust evaluation from indirect observation. Trust based routing is depicted in Section 3.5. The performance and effectiveness of our scheme are evaluated and discussed in Section 3.6. Finally, we conclude the work in Section 3.7.

3.2 Trust Model in MANETs

In this section, we describe the definition and properties of trust in MANETs. Based on the definition, we depict the trust model that is used to formulate the trust between two nodes in MANETs, and present a framework of the proposed scheme.

3.2.1 Definition and Properties of Trust

Trust has different meanings in different disciplines from psychology to economy [4, 64]. The definition of trust in MANETs is similar to the explanation in sociology, where trust is interpreted as degrees of the belief that a node in a network (or an agent in a distributed system) will carry out tasks that it should [4, 64]. Due to the specific characteristics of MANETs, trust in MANETs has five basic properties: subjectivity, dynamicity, non-transitivity, asymmetry, and context-dependency [4, 64]. Subjectivity means that an observer node has a right to determine the trust of an observed node. Different observer nodes may have different trust values of the same observed node. Dynamicity means that the trust of a node should be changed depending on its behaviors. Non-transitivity means that if node A trusts node B and node B trusts node C, then node A does not necessarily trust node C. Asymmetry

means that if node A trusts node B, then node B does not necessarily trust node A. Context-dependency means that trust assessment commonly bases on the behaviors of a node. Different aspects of actions can be evaluated by different trust. For example, if a node has less power, then it may not be able to forward messages to its neighbors. In this situation, the trust of power in this node will decline, but the trust of security in this node will not be changed due to its state.

Reputation is another important concept in trust evaluation. Reputation reflects the public opinions from members in a community [96]. In MANETs, reputation can be a collection of trust from nodes in the network. Reputation is more global than trust from the perspective of the whole network [96].

3.2.2 Trust Model

Based on the definition and properties of trust in MANETs, we evaluate trust in the proposed scheme by a real number, T, with a continuous value between 0 and 1. Although trust and trustworthiness may be different in contexts, in which the trustor needs to consider risk [4], trust and trustworthiness are treated the same for simplicity in the proposed scheme.

In this model, trust is made up of two components: direct observation trust and indirect observation trust. These components are similar to those used in [60]. In direct observation trust, an observer estimates the trust of his one-hop neighbor based on its own opinion. Therefore, the trust value is the expectation of a subjective probability that a trustor uses to decide whether or not a trustee is reliable. It is similar to first-hand information defined by [57, 69].

We denote T^S as a trust value from direct observation and can be calculated by Bayesian inference. The detailed explanation is in Section 3.3.

If we only consider direct observation, there would be prejudice in trust value

calculation. In order to obtain less biased trust value, we also consider other observers' opinions. Although opinions of neighbors are introduced in [60], the method that simply takes arithmetic mean of all trust values is not sufficient to reflect the real meaning of other unreliable observers' opinions because there are two situations that may severely disturb the effective evidence from neighbors: unreliable neighbors and unreliable observation [70]. Unreliable neighbors themselves are suspects. Even though neighbors are trustworthy, they may also provide unreliable evidence due to observation conditions. The Dempster-Shafer theory [14, 70] is a good candidate to aid in this situation, in which evidence is collected from neighbors that may be unreliable. Therefore, we denote the trust value derived from indirect observation of one-hop neighbors as T^N. Combining the trust value, T^S, from direct observation and the trust value, T^N, from indirect observation, we can get a more realistic and accurate trust value of a node in MANETs.

$$T = \lambda T^S + (1 - \lambda)T^N, \tag{3.1}$$

where λ is a weight assigned to T^S, $0 \leq \lambda \leq 1$.

3.2.3 Framework of the Proposed Scheme

Based on the trust model, the framework of the proposed scheme is shown in Fig. 3.1. In the trust scheme component, the module of trust evaluation and update can obtain evidence from direct and indirect observation modules and then utilize two approaches, Bayesian inference and DST, to calculate and update the trust values. Next, the trust values are stored in the module of trust repository. Routing schemes in the networking component can establish secure routing paths between sources and destinations based on the trust repository module. The application component can send data through secure routing paths.

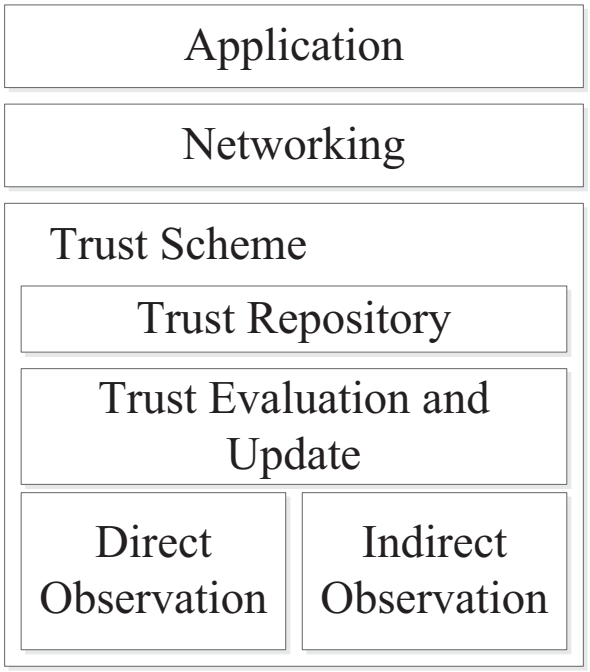

Figure 3.1: The framework of the proposed scheme.

The trust from direct observation between an observer node A and an observed node B in this trust scheme can be defined further as

$$T_{AB}^{S} = \rho T_{AB}^{D} + (1 - \rho) T_{AB}^{C}, \tag{3.2}$$

where ρ $(0 \leq \rho \leq 1)$is the weight for data packets; T_{AB}^{D} is the trust value based on data packets; T_{AB}^{C} is the trust value based on control packets. Trust from indirect observation between an observer node A and an observed node B, denoted as T_{AB}^{N}, can be obtained by DST, which will be explained in Section 3.4.

In order to explain the basic procedure of trust evaluation in our scenario, an example network is shown in Fig. 3.2. In this example, node 1 is an observer node and node 3 is an observed node. Node 1 sends data messages to node 5 through node

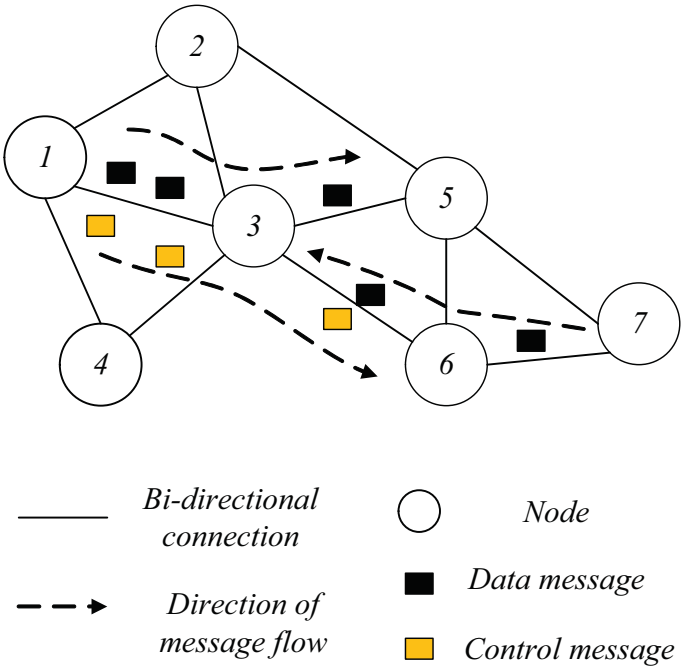

Figure 3.2: An example mobile ad hoc network.

3. When node 3 receives data messages and forwards to node 5, node 1 can overhear it. Then node 1 can calculate the trust value of node 3 based on data messages. The same idea is applied to the control message situation. In the meanwhile, node 1 can collect information from node 2 and node 4, which have interactions with node 3 in order to evaluate the trust value of node 3. This information collected from third party nodes is called indirect observation. In another situation, node 7 sends data messages to node 3, which is the destination node. Node 1 cannot overhear the data messages sent to node 3 in this situation.

3.3 Trust Evaluation with Direct Observation

Based on the model presented in the last section, we evaluate trust values with direct observation on two malicious behaviors: dropping packets and modifying packets [25]. In the direct observation, we assume that each observer can overhear packets

forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviors of the observed node. Therefore, the observer node can calculate trust values of its neighbors by using Bayesian inference, which is a general framework to deduce the estimation of the unknown probability by using observation [57, 80, 97]. As mentioned in the last section of trust model, the degree of belief is a random variable, denoted by Θ and $0 \leq \theta \leq 1$. From Bayes' theorem, we can derive the following formulation

$$f(\theta, y|x) = \frac{p(x|\theta, y)f(\theta, y)}{\int_0^1 p(x|\theta, y)f(\theta, y)\,\mathrm{d}\theta}, \tag{3.3}$$

where x is the number of packets is forwarded correctly; y is the number of packets is received by a node; $p(x|\theta, y)$ is the likelihood function, which follows a binomial distribution

$$p(x|\theta, y) = \binom{y}{x}\theta^x(1-\theta)^{y-x}. \tag{3.4}$$

We assume that the prior distribution, $f(\theta, y)$, follows Beta distribution,

$$Beta(\theta; \alpha, \beta) = \frac{\theta^{\alpha-1}(1-\theta)^{\beta-1}}{\int_0^1 \theta^{\alpha-1}(1-\theta)^{\beta-1}\,\mathrm{d}\theta}, \tag{3.5}$$

where $0 \leq \theta \leq 1, \alpha > 0, \beta > 0$. Then we have

$$f(\theta, y|x) \sim Beta(\alpha + x, \beta + y - x). \tag{3.6}$$

The expectation of Beta distribution is

$$E[\Theta] = \frac{\alpha}{\alpha + \beta}. \tag{3.7}$$

From (3.6), the trust value is calculated iteratively. At the beginning, there are no observation. The prior distribution $f(\theta, y)$ is $Beta(\theta; 1, 1)$ at the beginning. Then we have

$$E_n[\Theta] = \frac{\alpha_n}{\alpha_n + \beta_n}, \tag{3.8}$$

where $\alpha_n = \alpha_{n-1} + x_{n-1}, \beta_n = \beta_{n-1} + y_{n-1} - x_{n-1}, \alpha_0 = \beta_0 = 1, n \in \mathbb{Z}^+$. Intuitively, this situation is explained that the trust value of a node is 0.5 at the beginning. That means the node is seemed as neutral when no history records behaviors is established. The trust value can be revised continuously through follow-up observation.

Past experience is also an important factor when trust values are calculated. Recent activities of a node can seriously affect the trust evaluation. Consider the case where a node has a good history of past experience, but it drops or modifies packets recently. In order to handle this, a windowing scheme is proposed [57, 60]. Using weighted evidence from observation is another method [69].

In our scheme, we introduce a punishment factor for reputation fading, which focuses on recent activities. The punishment factor is used to give more weights on misbehavior in the Bayesian framework. Firstly, this can lower the trust of an attacker when it misbehaves. Secondly, the trust of the attack will not recover quickly even if it forwards a large number of packets correctly due to the impact of the punishment factor. This can help the proposed scheme distinguish the malicious node quickly and avoid them disrupting the normal traffic between benign nodes again. The punishment factor is inspired by our daily lives in human society, where a scandal can badly affect a person who has a good reputation. What's more, it is hard to quickly recover a good reputation. The factor of punishment makes the trust evaluation more realistic. The punishment factor, γ_n, in the formula of trust

evaluation is described as follows:

$$T^S = \frac{\alpha_n}{\alpha_n + \gamma_n \beta_n}, \tag{3.9}$$

where $\gamma_n \geq 1$. As the value of γ_n becomes larger, the trust value declines more. This is because the punishment factor gives more weight to misbehavior.

3.4 Trust Evaluation with Indirect Observation

In this section, indirect observation from neighbor nodes used to evaluate the trust value of the observed node will be discussed. Although direct observation from an observer is important in assessing the trust value of the observed node, the testimonies from neighbor nodes are also helpful to judge the trustworthiness of the observed node. Collection of neighbors' opinions can help in justifying whether or not a node is hostile. This mechanism may reduce the bias from an observer. A situation in which a node is benign to one node but malicious to others may be mitigated. In order to implement this method, the Dempster-Shafer theory, which is a mathematical theory of evidence, is used as it is well developed for coping with uncertainty or ignorance, and it provides a numerical measurement of degrees of belief about a proposition from multiple sources [15, 46]. The core of this theory is the belief function that is based on two essential ideas: degrees of belief about a proposition can be obtained from subjective probabilities of a related question, and these degrees of belief can be combined together on condition that they are from independence evidence [13, 70]. In the indirect observation, we assume that there are more than one neighbor nodes between an observer and an observed node when the trust evaluation is performed with DST. We also assume that evidence provided by different neighbors is independent.

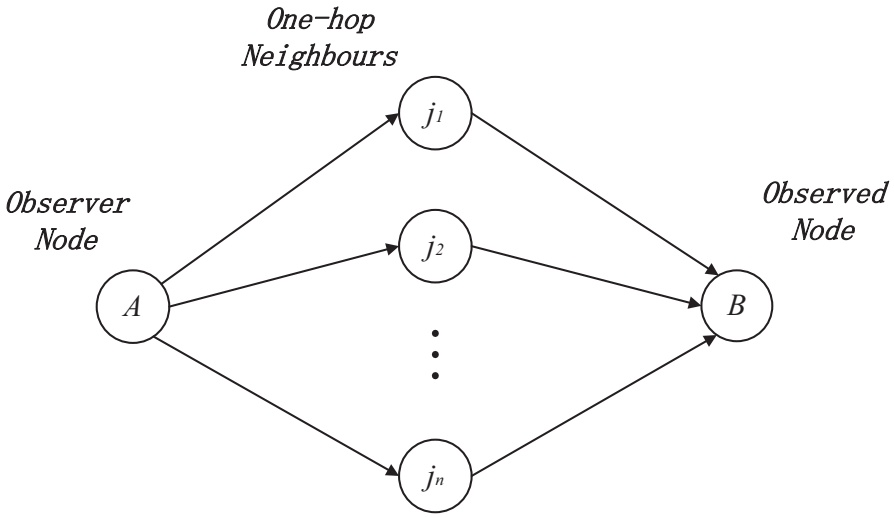

Figure 3.3: A scenario for indirect observation.

First, we will introduce the theory of belief functions. Then, we will discuss the rule of combining belief functions that are used to accommodate testimonies from one-hop neighbor nodes in order to assess trust values of nodes in MANETs.

3.4.1 Belief Function

In the Dempster-Shafer theory, a frame of discernment is a set of propositions that are mutually exclusive and exhaustive, which is denoted by Ω [70]. Based on the frame of discernment, the basic probability value of a focal set, A_i, is a function $m : 2^{\Omega} \longrightarrow [0, 1]$, which satisfies following conditions: $m(\emptyset) = 0$; and $\sum_{A_i \subseteq \Omega} m(A_i) = 1$. For any subset B of the frame of discernment, the belief function is defined as

$$bel(B) = \sum_{A_i \subseteq B} m(A_i). \tag{3.10}$$

In our scenario shown in Fig. 3.3, we designate two security states to a node, i.e., trustworthy and untrustworthy, which is similar to [14, 70]. Therefore, the frame of discernment in the Dempster-Shafer theory, $\Omega = \{trustworthy, untrustworthy\}$,

which demonstrates that node B has two states: trustworthy and untrustworthy. Node A evaluates the trust value of node B through one-hop neighbors between them. One-hop neighbors of node B can provide evidence to a subset of Ω with hypothesis H, i.e., node B is trustworthy. The power set of our scenario, 2^{Ω}, includes: $\varnothing$; hypothesis $H = \{trustworthy\}$; hypothesis $\overline{H} = \{untrustworthy\}$; and hypothesis $U = \Omega$, which means that the observed node B is either in the trustworthy state or untrustworthy state. Each one-hop neighbor gives evidence from its observation by assigning its beliefs over Ω. Each hypothesis is assigned a basic probability value $m(H)$ between 0 and 1. In our scheme, the basic probability value can be obtained from direct observation. For example, the trust value of node j_1 is $T^S_{Aj_1}$, from direct observation of node A to node j_1. If node j_1 believes that node B is trustworthy, then the basic probability value $m_{j_1}(H)$ is $T^S_{Aj_1}$. The basic probability value $m_{j_1}(\overline{H})$ is 0. From the definition of belief function, $m_{j_1}(U)$ is equal to $1 - T^S_{Aj_1}$. The formulae are as follows [70]:

$$\begin{aligned} m_{j_1}(H) &= T^S_{Aj_1}, \\ m_{j_1}(\overline{H}) &= 0, \\ m_{j_1}(U) &= 1 - T^S_{Aj_1}, \end{aligned} \tag{3.11}$$

If node j_1 believes that node B is untrustworthy, the formulae are as follows:

$$\begin{aligned} m_{j_1}(H) &= 0, \\ m_{j_1}(\overline{H}) &= T^S_{Aj_1}, \\ m_{j_1}(U) &= 1 - T^S_{Aj_1}, \end{aligned} \tag{3.12}$$

The belief function of each focal set can be obtained from (3.10). For example,

$$\begin{aligned} bel_{j_1}(H) &= m_{j_1}(H), \\ bel_{j_1}(\overline{H}) &= m_{j_1}(\overline{H}), \\ bel_{j_1}(U) &= m_{j_1}(H) + m_{j_1}(\overline{H}) + m_{j_1}(U). \end{aligned} \tag{3.13}$$

This means that from the testimony of node j_1, node A can derive whether or not node B is trustworthy based on the trust value of node j_1.

3.4.2 Dempster's Rule of Combining Belief Functions

Based on the above description of belief function, Dempster-Shafer theory combines multiple neighbor nodes' belief on the condition that evidence from different neighbor nodes is independent [14, 70]. Assuming that $bel_1(B)$ and $bel_2(B)$ are two belief functions over the same frame of discernment, Ω, the orthogonal sum of $bel_1(B)$ and $bel_2(B)$, $bel(B)$, is defined as

$$\begin{aligned} bel(B) &= bel_1(B) \oplus bel_2(B) \\ &= \frac{\sum_{i,j,A_i \bigcap A_j = B} m_1(A_i) m_2(A_j)}{\sum_{i,j,A_i \bigcap A_j \neq \varnothing} m_1(A_i) m_2(A_j)}, \end{aligned} \tag{3.14}$$

where $A_i, A_j \subseteq \Omega$. The order of the combination of belief functions does not affect the result value produced by Dempster' rule due to the commutativity of multiplication [14].

In our scenario, we assume that there are one-hop neighbors beside node B as shown in Fig. 3.3. Therefore, the combined belief of node j_1 and node j_2 is calculated as follows [70]:

$$
\begin{aligned}
m_{j_1}(H) \oplus m_{j_2}(H) &= \frac{1}{K}[m_{j_1}(H)m_{j_2}(H) \\
&\quad +m_{j_1}(H)m_{j_2}(U) \\
&\quad +m_{j_1}(U)m_{j_2}(H)], \\
m_{j_1}(\overline{H}) \oplus m_{j_2}(\overline{H}) &= \frac{1}{K}[m_{j_1}(\overline{H})m_{j_2}(\overline{H}) \\
&\quad +m_{j_1}(\overline{H})m_{j_2}(U) \\
&\quad +m_{j_1}(U)m_{j_2}(\overline{H})], \\
m_{j_1}(U) \oplus m_{j_2}(U) &= \frac{1}{K}m_{j_1}(U)m_{j_2}(U),
\end{aligned} \tag{3.15}
$$

where

$$
\begin{aligned}
K &= m_{j_1}(H)m_{j_2}(H) + m_{j_1}(H)m_{j_2}(U) \\
&\quad +m_{j_1}(U)m_{j_2}(U) + m_{j_1}(U)m_{j_2}(H) \\
&\quad +m_{j_1}(U)m_{j_2}(\overline{H}) + m_{j_1}(\overline{H})m_{j_2}(\overline{H}) \\
&\quad +m_{j_1}(\overline{H})m_{j_2}(U).
\end{aligned} \tag{3.16}
$$

For instance, assuming that

$$
\begin{aligned}
&m_{j_1}(H) = 0.8, m_{j_1}(\overline{H}) = 0, m_{j_1}(U) = 0.2, \\
&m_{j_2}(H) = 0.7, m_{j_2}(\overline{H}) = 0, m_{j_2}(U) = 0.3,
\end{aligned}
$$

then we can obtain the result of combining two belief functions as follows:

$$
\begin{aligned}
bel(H) &= 0.8 * 0.7 + 0.8 * 0.3 + 0.7 * 0.2 = 0.94 \\
bel(\overline{H}) &= 0 * 0 + 0 * 0.3 + 0 * 0.2 = 0 \\
bel(U) &= 0.2 * 0.3 = 0.06
\end{aligned}
$$

That means from the result of combination, the trust value of node B from indirect observation is 0.94.

Following the rule of combination of belief, we can combine more results from neighbor nodes. Based on the Dempster-Shafer theory, T_{AB}^{N} is defined as:

$$T_{AB}^{N} = m_{j_1}(H) \oplus m_{j_2}(H) \ldots \oplus m_{j_n}(H), \tag{3.17}$$

where node j_i, $1 \leq i \leq n$, is an one-hop neighbor of node A and node B.

3.5 Secure Routing Based on Trust

The original OLSRv2 [6] does not provide security measurements in the protocol. OLSRv2 assumes that every node is cooperative and benevolent. However, this assumption is inappropriate in a military environment. Malicious nodes can attack nodes that are not protected. Based on trust values, a secure route can be established.

Modifications of OLSRv2 include two important parts: route selection process based on link metrics and trust value calculation algorithms. Although OLSRv2 provides new features such as link metrics and extensible message formats, which may be used to improve security of the protocol, OLSRv2 implementation [6] [98] still attempts to use hop count when the shortest routing path is calculated. In order to implement route selection process based on link metrics, there are three components that need to be changed, HELLO and TC messages, protocol information bases, and the shortest path algorithm. Message format is extensible and flexible in OLSRv2. Thus link metrics information can be added to messages as Type Length Value (TLV) blocks. Modification of protocol information bases, including local information base,

neighbor information base and topology information base, is used to record link metrics in each node. Based on these information bases, route processing set can update the shortest routing path with link metrics. The detailed description of the modification of route selection process based on link metrics is shown in [99].

Based on the Internet draft of OLSRv2 [6], there are two types of control messages, HELLO and TC. In this trust management, we only consider the TC messages because of the need for forwarding TC. The message type of TC, which is defined in OLSRv2 Internet draft, can be used to check the type of the message. The trust management scheme can separate the data and control messages by the message type during trust evaluation. For other standard protocols, like AODV [21], the trust management scheme also can differentiate the control messages, e.g., RREQs, RREPs in AODV, by message type checking when a trust evaluation procedure is performed.

We assume that each node works in the promiscuous mode implemented by the MAC layer. We also assume that, in a time slot, the observed node (sender) does not move out of the transmission range. As the time of packets processing in a node is short, our assumptions are realistic in practical networks. This means that the observer can detect whether or not the neighboring node sends the received packets before the observed node moves out the transmission range.

Every node needs to record its one-hop neighbors, how many data packets each neighbor received, how many control packets each neighbor received, how many data packets each neighbor forwards correctly, and how many control packets each neighbor forwards correctly. In OLSRv2, there are two types of control messages: HELLO and TC. TC message is only recorded for trust evaluation because HELLO message is transmitted with one hop in the network. When a node receives a packet, the number of received packets, according to the type, will increase one. If the node forwards the received packet correctly, the number of forwarded packets will increase

Algorithm 1 Trust Calculation with Direct Observation

```
1: if node A, which is an observer, finds that its one-hop neighbor, Node B that is
   a trustee, receives a packet then
2:    the number of packets received increases one
3:    if node A finds that node B forwards the packet successfully then
4:       the number of packets forwarded increases one
5:    else
6:       if TTL of the packet becomes zero or overflow of buffers in node B or the
         state of wireless connection of node B is bad then
7:          the number of packets received decreases one
8:       end if
9:    end if
10: end if
11: calculate the trust value, T^S, from (3.9) and update the old one.
```

one. There are three scenarios that the number of received packets will not increase. Firstly, if the packet is dropped because of time to live (TTL), then the number of received packets should not increase. Secondly, if a node that receives a packet drops it due to overflow of buffers. Thirdly, a packet is dropped by a node because the state of wireless connection is bad. Considering these significant factors, we improve the accuracy of trust calculation.

We consider the condition that packets are dropped due to unreliable wireless connections. During the trust evaluation with direct observation, the scheme can remove the number of packets dropped by this condition (in Algorithm 1). We assume that there is a probability that packets are dropped because of unreliable wireless connections. Algorithm 1 depicts the details of each iteration. Algorithm 2 describes that an observer node collects evidence from its one-hops neighbors between the observer node and the observed node. Then the trust values from indirect observation are evaluated by (3.17). After T^S and T^N are obtained, we can get the total trust value of the observed node by (3.1). In proactive routing protocols, such as OLSRv2, an observer node can obtain the information from its neighbor nodes periodically by control messages (e.g., HELLO and TC), which can be used to carry the trust values.

Algorithm 2 Trust Calculation with Indirect Observation

if node A, which is an observer, has more than one one-hop neighbors between it and the trustee, node B **then**
  calculates the trust value, T^N, from (3.17)
else
  set T^N to 0
  set λ to 1
end if

Compared to the existing OLSRv2 scheme that uses the shortest path based on hop count, we derive the best routing path considering both trust values and hop count. Here we will explain how to derive a route trust value from node trust values. We use the Dijkstra' algorithm to calculate the best routing path with trust. Since minimization is used in the Dijkstra' algorithm (e.g., to find the shortest path with the minimal hop count in traditional OLSRv2), we need to convert the trust value of each node in the routing path to untrustworthy value. Then, we can minimize the untrustworthy value of a path using the Dijkstra' algorithm. To this end, we define the untrustworthy value between node A and node B as U_{AB}, which can be calculated as $U_{AB} = 1 - T_{AB}$. The sum of untrustworthy values of a routing path is

$$U_{path} = \sum_{i=1}^{n-1} U_{k_i k_{i+1}} = \sum_{i=1}^{n-1} (1 - T_{k_i k_{i+1}}), \tag{3.18}$$

where $T_{k_i k_{i+1}}$ is the trust value between node k_i and its one-hop neighbor, node k_{i+1}. Nodes k_1, k_2, ..., k_n belong to the path with $n-1$ hops. The most trustworthy routing path is the path that satisfies the minimum of U_{path}. In other words, the routing path is comprised of the smallest number of nodes with high trust values.

The trust values and routing table of each node can be stored in the Trust Platform Module (TPM) [100], which provides additional security protection in open environments with the combination of software and hardware. Since the trust values in each node are the key facilities to detect malicious nodes, the TPM is able to

provide effective protection to secure routing to avoid malicious attacks by enemies in battlefields.

3.6 Simulation Results and Discussions

The proposed scheme is simulated on the Qualnet [7] platform with the OLSRv2 protocol [6, 98]. In the simulations, the effectiveness of the scheme is evaluated in an insecure environment. We compare the performance of the proposed scheme with that of OLSRv2 without security mechanisms.

3.6.1 Environment Settings

We randomly place nodes in the defined area. Each scenario has a pair of nodes as the source and destination with Constant Bit Rate (CBR) traffic. The simulation parameters are listed in Table 3.1. In our simulations, we assume that there are two types of nodes in the network: normal nodes, which follow the routing rules, and compromised nodes, which drop or modify packets maliciously. There are 5 nodes in the $300m \times 300m$ area, 10 nodes in the $500m \times 500m$ area, 15 and 20 nodes in the $800m \times 800m$ area, and 25 and 30 nodes in the $1000m \times 1000m$ area. We also assume that the number of compromised nodes is minor compared to the total number of nodes in the network. The faction of malicious nodes is from 1/5 to 1/3. In this adversary mode, the proposed scheme is evaluated and compared with the original OLSRv2 protocol. We have simulated networks with different numbers of nodes. Fig. 3.4 is an example of the network setup where node 1 is the source node that generates the CBR traffic, node 3 is the destination node, and node 2 is compromised by an adversary. For node mobility, the random waypoint mobility model is adopted in a 30-node MANET. The maximum velocity of each node is set from 0 to 10 m/s. The

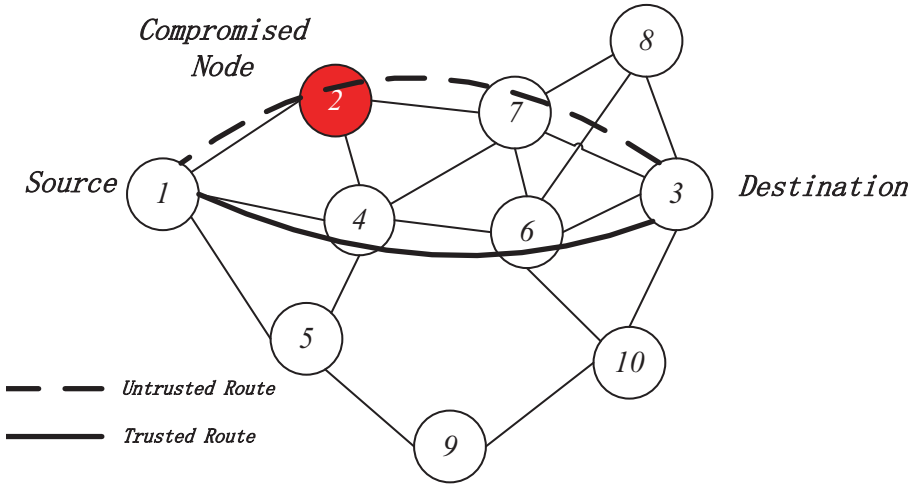

Figure 3.4: An example of the network setup.

pause time is 30 seconds. The simulation is repeated more than 30 times.

There are five performance metrics [101] considered in the simulations: 1) *Packet delivery ratio (PDR)* is the ratio of the number of data packets received by a destination node and the number of data packets generated by a source node; 2) *Throughput* is the total size of data packets correctly received by a destination node every second; 3) *Average end-to-end delay* is the mean of end-to-end delay between a source node and a destination node with CBR traffic; 4) *Message Overhead* is the size of Type Length Value (TLV) blocks in total messages, which are used to carry trust values; 5) *Routing load* is the ratio of the number of control packets transmitted by nodes to the number of data packets received successfully by destinations during the simulation.

3.6.2 Performance Improvement

The original OLSRv2 and our scheme are evaluated in the simulations, where some nodes misbehave through dropping or modifying packets. In Fig. 3.5, we compare our scheme with and without indirect observation and original OLSRv2 in scenarios that a source node sends data packets to a destination node in the network, which

Table 3.1: Simulation Parameters

Parameter	**Value**
Application protocol	CBR
CBR transmission time	1s to 100s
CBR transmission interval	0.5s
Packet size	512 bytes
Transport protocol	UDP
Network protocol	IPv4
Routing protocol	OLSRv2
MAC protocol	IEEE 802.11
Physical protocol	IEEE 802.11b
Data rate	2Mbps
Transmission power	6dBm
Radio range	180m
Propagation pathloss model	Two-ray
Simulation area	300m × 300m, 500m × 500m, 800m × 800m, 1000m × 1000m
Number of nodes	5, 10, 15, 20, 25, 30
Simulation time	300s

includes nodes from 5 to 30.

From Fig. 3.5, we can see that the proposed scheme has a much higher PDR than the existing scheme because the trust based routing calculation can detect the misbehavior of malicious nodes. The results also demonstrate that the proposed scheme with indirect observation has the highest PDR among these three schemes. In Fig. 3.5, we also can find that the PDR of three schemes decreases gradually when the number of nodes grows. This is because the collision of sending messages becomes more frequent as the number of nodes increases in the MANET. Although the PDR declines in three schemes, the proposed scheme is apparently better than the existing scheme. In Fig. 3.6, we evaluate throughput in our scheme and the original one. Although the number of packets received correctly decreases as long as the number of nodes increases, the performance of our scheme has a big improvement. Fig. 3.5 and Fig. 3.6 both reveal that the trust based routing algorithm can improve the performance of OLSRv2. Fig. 3.7 and Fig. 3.8 show the impact of node mobility in a 30-node MANET. We can observe that, as the node velocity increases, PDR and throughput decrease gradually. This is because the higher speed of a node may increase the probability of packets lost. Nevertheless, the proposed scheme has better performance than the existing one.

The number of malicious nodes in the MANET also has a significant impact on the throughput of the network. Here, we assume the attackers are independent. Hence, there is no collusion attack in the MANET. We investigate the throughput with malicious nodes, from 2 to 10, in a 30-node MANET environment. The basic parameter is the same as above. Fig. 3.9 shows that, as the number of malicious nodes increases, the throughput drops dramatically. When the number of malicious nodes reaches to one third of the total number of nodes in the network, the throughput decreases to about half of the throughput in the network with 2 malicious nodes. From

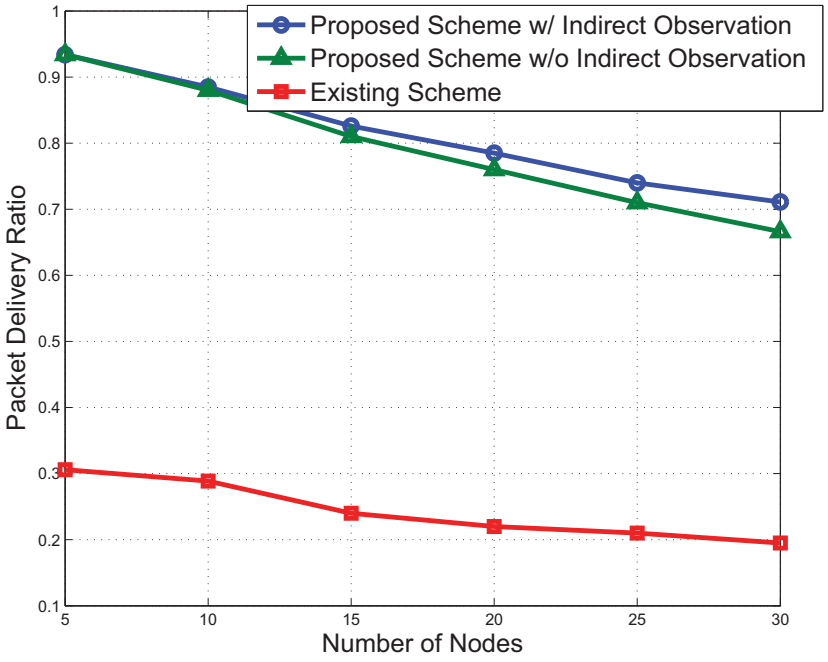

Figure 3.5: Packet delivery ratio (PDR) versus the number of nodes in the network.

this figure, we can see that the proposed scheme is affected deeply by the number of malicious nodes. Compared to the proposed scheme, the existing scheme has a very low throughput even if the number of malicious nodes is very small.

From Fig. 3.5 to Fig. 3.8, we can observe that our proposed scheme based on trust outperforms the existing scheme significantly in terms of both PDR and throughput. Our scheme takes advantage of trust evaluation of nodes in the network so that more reliable routing paths can be established. The existing scheme is severely affected by malicious nodes that drop or modify packets. We can observe that the proposed scheme with trust can steer clear of malicious nodes dynamically. Therefore, the PDR and throughput of our scheme are better than those of the existing scheme.

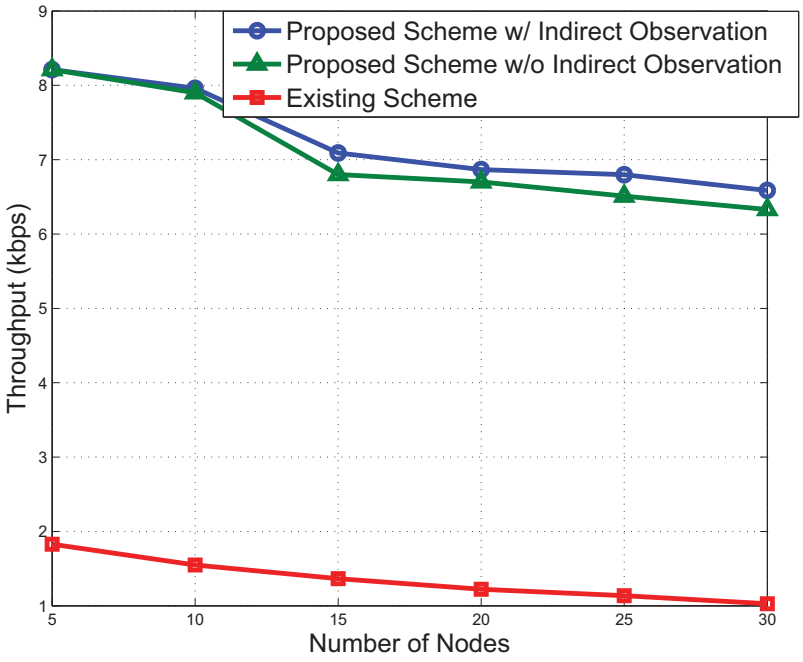

Figure 3.6: Throughput versus the number of nodes in the network.

3.6.3 Cost

The cost of security enhancement in OLSRv2 mainly includes the increased average end-to-end delay and overhead of messages that are used to carry trust values of nodes. Fig. 3.10 shows that the proposed scheme has a slightly higher average end-to-end delay than the existing scheme in the malicious environment. In Fig. 3.11, we can see that, as the node velocity increases, the average end-to-end delay becomes longer. The reason is that trust based routing path is usually a longer route from a source node to a destination node. Therefore, there is a trivial delay introduced by the proposed scheme. Nevertheless, higher security is guaranteed in the proposed scheme.

Compared to local computing capacity, sending and receiving message is an important issue in MANETs because message transmission is energy-consuming. Thus,

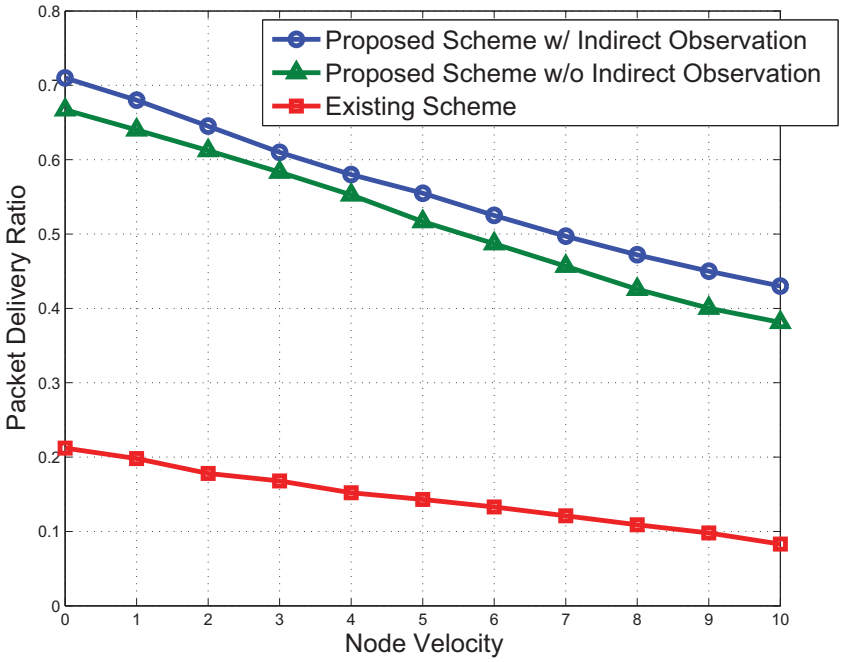

Figure 3.7: Packet delivery ratio versus node velocity.

we study how much overhead of messages is imported when the trust value is calculated in the OLSRv2 protocol. Since the metric link value is introduced in OLSRv2, one new address block TLV, which occupies 12 bytes, is added to the message format described in Section 3.5. Fig. 3.12 shows how much the overhead of messages is imported compared to the original version of OLSRv2. Because trust values are embedded in the HELLO messages and TC messages, there is no more messages need to be sent. The overhead is not very high. However, as the number of nodes increases, the percentage of overhead in messages drops dramatically, as shown in Fig. 3.13. This is because, when the number of nodes increases, the total message becomes large. Then the 12-byte overhead is trivial compared to the size of messages. In Fig. 3.14, the results demonstrate that the proposed scheme has a lower routing load because of the higher number of packets received correctly by the destination node. As the number of nodes increases, the routing load of the existing and proposed schemes

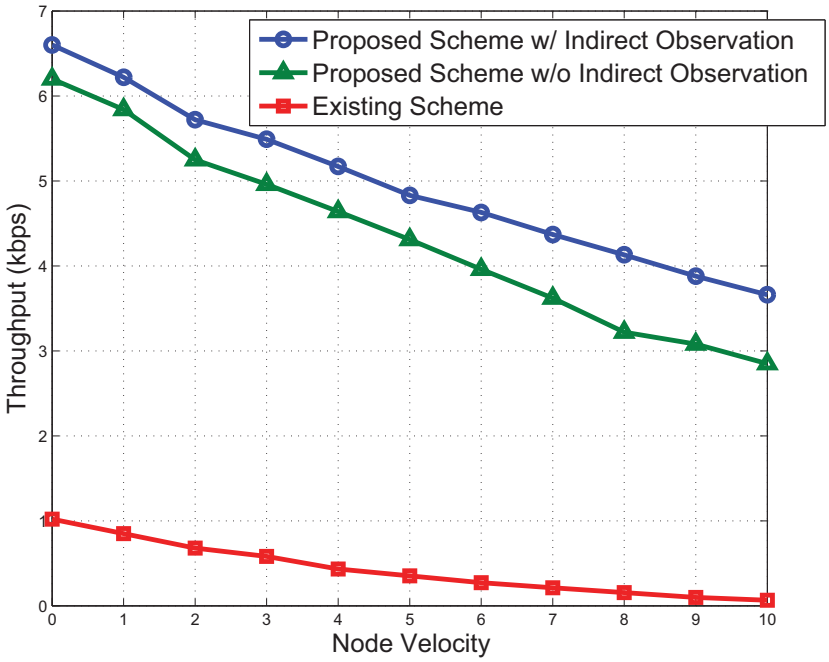

Figure 3.8: Throughput versus node velocity.

climb up due to the nature of proactive routing protocol: periodical generation of control messages in every node.

3.7 Chapter Summary

In this part, we proposed a unified trust management scheme that enhances the security of MANETs. Using recent advances in uncertain reasoning, Bayesian inference and Dempster-Shafer theory, we evaluate the trust values of observed nodes in MANETs. Misbehaviors such as dropping or modifying packets can be detected in our scheme through trust values by direct and indirect observation. Nodes with low trust values will be excluded by the routing algorithm. Therefore, secure routing path can be established in malicious environments. Based on the proposed scheme,

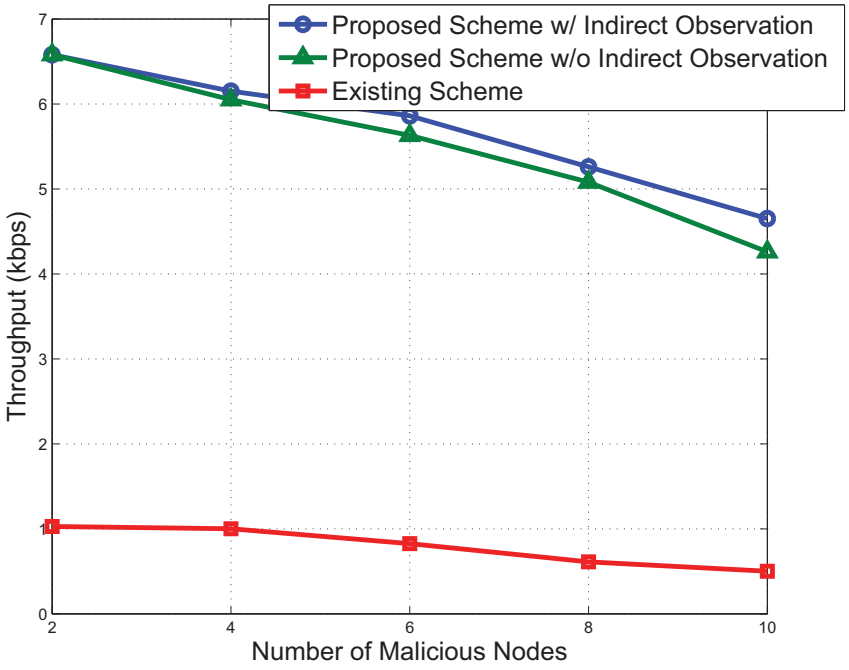

Figure 3.9: Throughput versus the number of malicious nodes in the network.

more accurate trust can be obtained by considering different types of packets, indirect observation from one-hop neighbors and other important factors such as buffers of queues and states of wireless connections, which may cause dropping packets in friendly nodes. The results of MANET routing scenario positively support the effectiveness and performance of our scheme, which improves throughput and packet delivery ratio considerably, with slightly increased average end-to-end delay and overhead of messages.

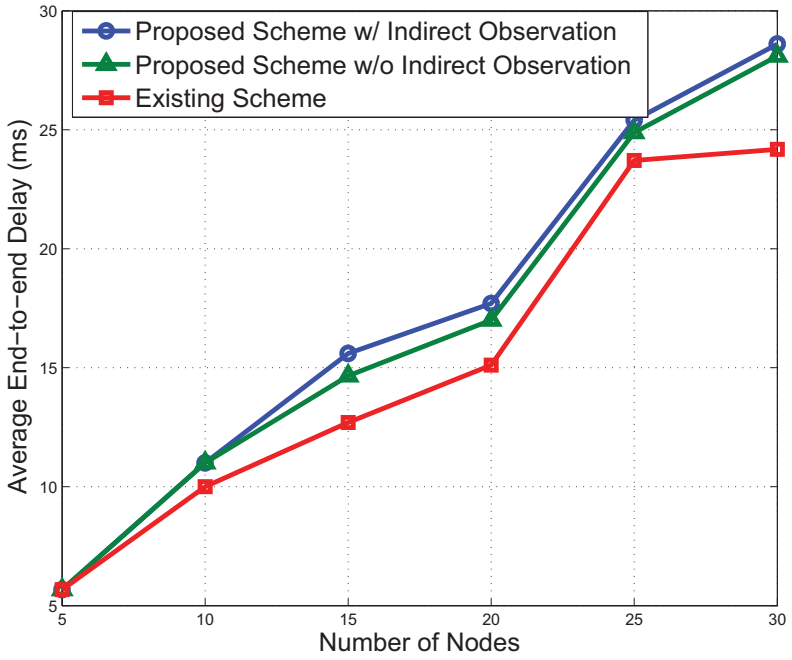

Figure 3.10: Average end-to-end delay versus the number of nodes in the network.

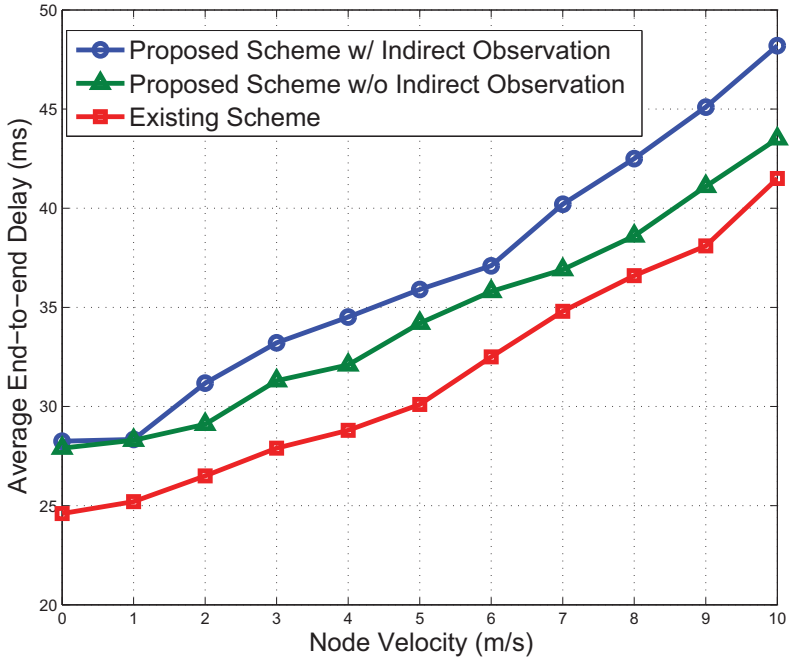

Figure 3.11: Average end-to-end delay versus node velocities.

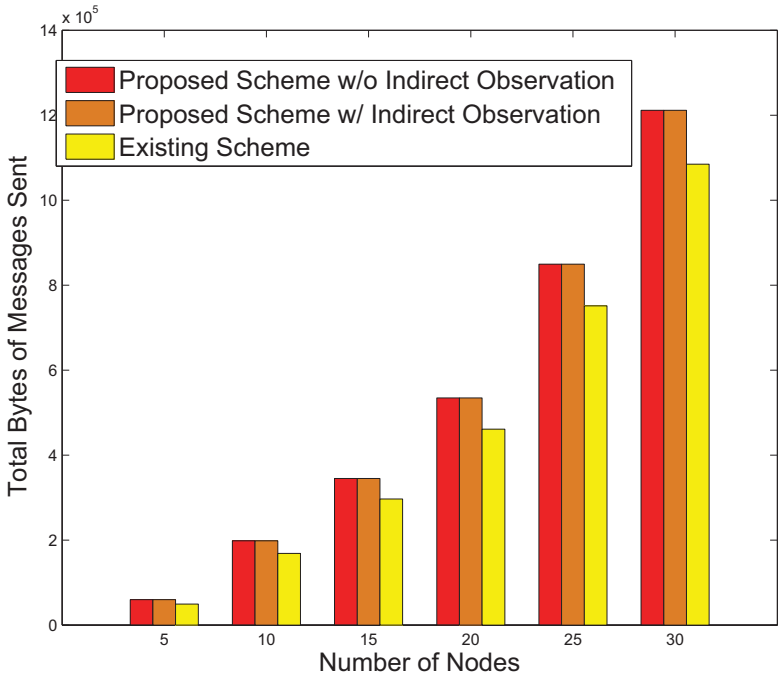

Figure 3.12: Total bytes of messages sent versus the number of nodes in the network.

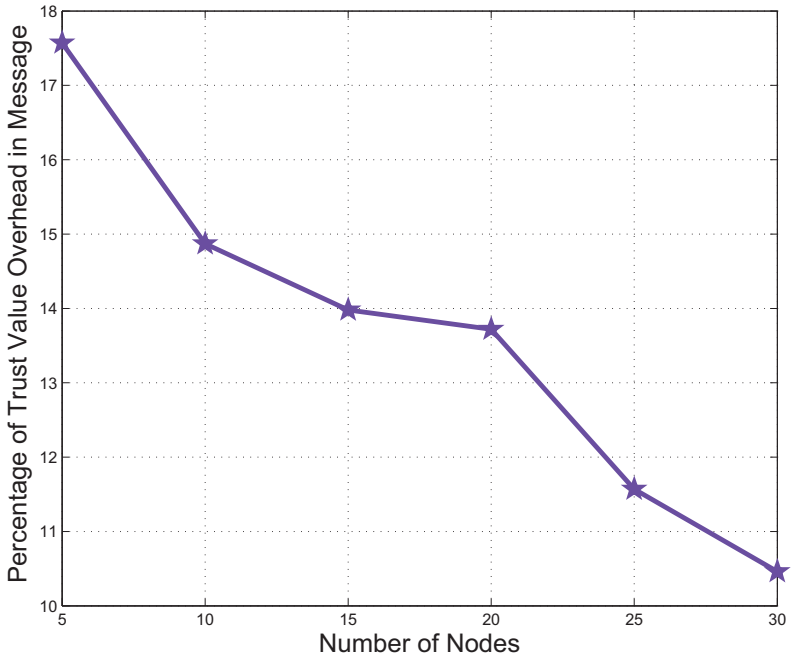

Figure 3.13: Percentage of overhead in message versus the number of nodes in the network.

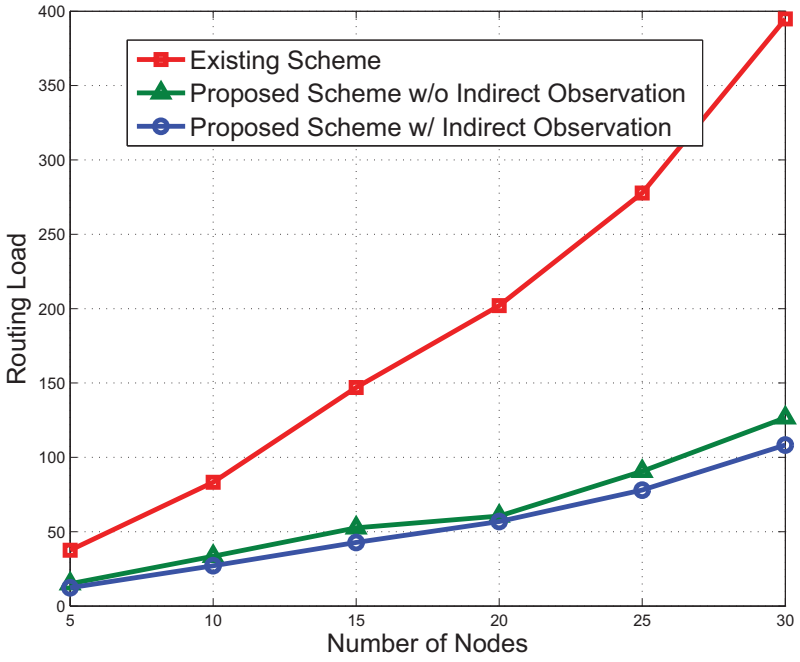

Figure 3.14: Routing load versus the number of nodes in the network.

Chapter 4

Trust Management with Bayesian Networks

This chapter is organized as follows. Section 4.2 depicts the network model and the attack model. Section 4.3 describes a security scheme with trust using Bayesian networks. The performance and effectiveness of our scheme are evaluated and discussed in Section 4.4. Finally, we conclude the work in Section 4.5.

4.1 Introduction

MANETs are a type of temporal and self-organized networks, which are suitable for tactical environments and disaster recovery scenarios [19]. Due to its distinguishing characteristics, e.g., no requirements of infrastructure, MANETs have been attracting a lot of attention. In this type of networks, nodes can form a distributed network and communicate with each other via wireless medium. Each node has to cooperate with other nodes in order to deliver traffic from source nodes to destination nodes. The flexibility of MANETs make themselves suitable for tactical environments and disaster recovery situations, in which communication infrastructure cannot be established easily and immediately. However, MANETs are originally devised under an implicit

assumption that all nodes in MANETs are cooperative and benign. Once adversaries join in MANETs, the primary advantages of MANETs may become obvious vulnerabilities that can be attacked by malicious nodes due to the open and distributed nature of MANETs [102–104].

There are many attacks that can be performed more easily in MANETs than in fixed-infrastructure networks [18, 105]. Spoofing attacks, in which a node can masquerade as another node, usually happen in MANETs due to the lack of a centralized authority. Another well-known attack is the wormhole attack, in which two nodes collude to establish a "tunnel" between a source node and a destination node. Packets dropping attacks are known as black hole attacks, which do not forward packets for other nodes. Modification attacks commonly alter the fields of packets in order to cause traffic disorder. These attacks can damage MANETs applications. In order to mitigate threat for MANETs, some researchers had presented a variety of cryptographic methodologies, also named hard protection, to safeguard MANETs. Hard protection can effectively thwart attacks from outside of networks [18, 105]. However, as attackers become more and more intelligent and diverse, hard protection cannot prevent all attacks, especially inside attacks. Researchers inspired by lessons learned from security of wired networks recently begin to focus on soft protection for MANETs, e.g., trust-based schemes [18, 105, 106].

Trust in MANETs is different from traditional disciplines from psychology to management science, which has five distinct properties: subjectivity, dynamicity, intransitivity, context-awareness, and asymmetry [4]. Due to the uncertain nature of trust, it is quite challenging to evaluate the trust of a node in MANETs. As the advancement with artificial intelligence, Bayesian networks invented by Dr. Judea Pearl [12] can provide a feasible approach to tackle this uncertainty in trust. In Bayesian networks, there are three primary aspects [107]: subjective knowledge and

information are reflected in the graphical structure; inference of belief is under the conditional probability by Bayes's rule; causal reasoning between the domain variables is conducted in the graphical structure.

In previous works, researchers use Bayesian networks to combine different dimension trust [9–11]. In this chapter, we emphasize on causal reasoning that can facilitate trust evaluation considering the causes of attacks. Additionally, establishment of causal relationships in Bayesian networks can help us make predictions in the presence of interventions [8]. Our scheme uses causal reasoning on the Bayesian networks to evaluate the trust of nodes. The accurate trust value considering malicious intention can be deduced. Through simulations, we show that the proposed scheme has a better performance in trust evaluation comparing to existing schemes.

4.2 System Model

In this section, we introduce the network model used in this chapter and then present the packet dropping and modification attacks. The Bayesian network model is introduced at last.

4.2.1 Network Model

In this part, we consider a small scale MANET where nodes are connected and kept staying in the network. There are one hop or more between source nodes and destination nodes. We assume that the routing algorithm of the network is a proactive routing scheme, e.g., link state routing algorithm. That means each node in the MANET has a global view of the network topology. We assume that the communication links between nodes are not reliable due to environment factors with a pre-defined initial probability. Based on the advanced channel techniques and MAC layer schemes, we

also assume upper layers can collect the wireless link reliability.

4.2.2 Attack Model

Packet dropping attacks and modification attacks are two attacks considered. Packet dropping attacks can be classified into two types based on the intention of attackers: selfish attacks and malicious attacks. In selfish attacks, some nodes don't forward partial packets for other nodes because of its energy constraints. In malicious attacks, nodes don't forward packets due to its hostile nature. For a malicious attacker, three attack patterns can be adopted: maximum, on-off, random [108]. In the maximum pattern, a malicious attacker does its best to drop any packets that need to be forwarded in order to block all the traffic. This attack can be detected more easily compared to two other patterns. In the on-off pattern, an attack drops and forwards packets followed by a fixed schedule. Once the defence system learns the schedule, this attack can be thwarted effectively. The random attack pattern is the hardest one to be detected due to its uncertainty and unpredictability. Due to the characteristics of MANETs, this attack can be performed stealthily. Modification attacks mean that an attacker deliberately alters the fields in the packets. These attacks tend to disrupt the normal control information in order to block the network traffic or increase transmission delays [105].

4.2.3 Bayesian Networks

In order to explain how to use Bayesian networks to manage trust in MANETs, we need to present the basic concepts and idioms in Bayesian networks here. Bayesian networks are a type of graphical models that can efficiently represent the joint probability distribution for a large set of variables, which may have relationships with each other [8]. In other words, Bayesian networks are a combination of probability and

graph theories, meanwhile associated with inductive logic [109]. In order to analyze and evaluate trust with a Bayesian network, we need to follows three steps [107]: defining a set of state variables and its domains, establishing a directed acyclic graph to connect these variables, and obtaining and calculating conditional probability distributions associated with these variables.

In a Bayesian network, each vertex in the direct acyclic graph (DAG) represents a state variable, which describes a proposition in a context. The domain of a state variable can be discrete or continuous. We assume that all domains are discrete. Each state variable is represented by two bold capital letters. The direct links between vertices denote direct probabilistic interactions between them, mostly interpreted as causal connections (not necessarily) [110]. The direction of each link is from a parent node to a child node. Each vertex has an associated conditional probability distribution (CPD). Vertices with no parents have CPDs given any events. Based on Bayesian networks, the joint probability of all state variables is calculated by the chain rule [109],

$$P(\mathbf{X}) = \prod_{x \in \mathbf{X}} P(x|parent(x)), \tag{4.1}$$

where $\mathbf{X}$ is a set of state variables in a Bayesian network; $parent(x)$ denotes parent nodes of x in the Bayesian network.

There are three basic vertex connection types,which are cornerstones of Bayesian networks: sequential, diverging, and converging connections [111]. In Fig. 4.1, A is the parent of B and B is the parent of C. This structure of A, B, and C is defined as sequential connection in Bayesian Networks. The property of sequential connection is that if B is known, then A and C are independent. Mathematically,

$$P(A, C|B) = P(A|B)P(C|B). \tag{4.2}$$

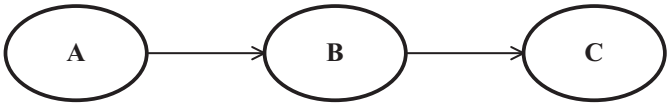

Figure 4.1: Sequential connection in a Bayesian network.

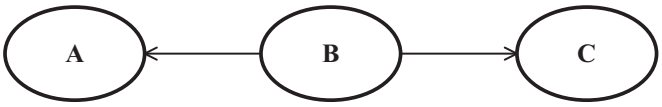

Figure 4.2: Diverging connection in a Bayesian network.

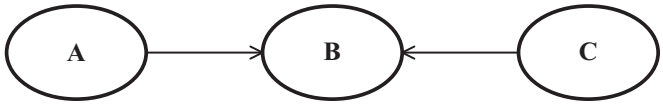

Figure 4.3: Converging connection in a Bayesian network.

In Bayesian networks terminology, A and C are d-separated given B [111]. Fig. 4.2 shows diverging connection, in which B is the parent of A and C. if B is given, then A and C are d-separated. Converging connection is presented in Fig. 4.3. In this connection, B is the child of A and C. The property of converging connection is different from other two connections. If the child, B, is known, then A and C are dependent. In Bayesian networks terminology, A and C are d-connected given B [111]. Based on these three basic connections, a complex Bayesian network, used to model trust in MANETs, can be established.

4.3 Trust Establishment in MANETs

In this section, we explain several terms in trust management at first. We then explain trust establishment via Bayesian networks.

Table 4.1: Variables in the Bayesian Network

Variable	Domain	CPD
Ma	$Val(Ma) = \{true, false\}$	$P(Ma)$
Wi	$Val(Wi) = \{high, low\}$	$P(Wi)$
Bu	$Val(Bu) = \{true, false\}$	$P(Bu)$
Mo	$Val(Mo) = \{true, false\}$	$P(Mo\|Ma)$
Dr	$Val(Dr) = \{true, false\}$	$P(Dr\|Ma, Wi, Bu)$
Tr	$Val(Tr) = \{high, medium, low\}$	$P(Tr\|Ma)$

4.3.1 Trust Establishment

In order to evaluate trust, we need to clearly distinguish several concepts that are related to trust. The first concept is experience with interactions, which is defined as two types of experience: experience from self and experience from others. Experience from self is a type of subjective belief that can be used to evaluate trust. Self experience can be obtained from direct interaction between two entities. Experience from others is defined as reputation [11, 96], which sometimes introduces confusion and is not distinguished from trust clearly in literature. Another concept related to trust is recommendation, which is always used in e-commerce systems [112]. Here we define recommendation as opinions from other entities that are trusted or not. Reputation can be obtained by recommendation from other entities. Finally, we need to mention that trust and trustworthiness are the same, albeit they are different in many other disciplines, e.g., sociology.

Trust Evaluation by Self Experience with a Bayesian Network Model

Traditionally, trust evaluation of a node is directly connected to the number of packets received and forwarded successfully [57]. Assuming packet dropping entirely caused by malicious nature of a node may not be realistic in MANETs. Because many other

factors, such as unreliable wireless connections and buffer overflows, can also cause packet dropping. Trust evaluation, which only depends on the statistics of dropping packet, is easy to decrease the trust of a node that is not malicious. The false trust of a node can heavily impact the performance of MANETs. Therefore, the trust of a node due to maliciousness needs to be calculated accurately. Further reasoning with packet dropping is needed in this situation. Reasoning also provides a venue to dynamic changes of uncertainty, which reflects the nature of trust in MANETs. The Bayesian Network is a good candidate for solving this problem due to its advantages [109]. Probabilistic description can handle the uncertainty of trust. Causal relations between the events can distinguish the causes of attacks. Dynamic updating can make trust evolve based on new evidence in order to obtain trust accurately and timely. Context information and knowledge can be processed efficiently and effectively by Bayesian statistical techniques [109].

In this chapter, we use a Bayesian network to analyze the intention of nodes in MANETs in order to accurately evaluate trust of each node. The trust establishment based on a Baysian network can differentiate these behaviors from malicious activities so that trust values of a node can be improved. Although there are many factors that may cause dropping packets, only the major factors include maliciousness, wireless connections, and buffer conditions, are listed here for simplicity. Meanwhile, other factors are trivial in this situation. If new factors are becoming significant, they can be added to the Bayesian network easily.

Following the steps mentioned before, we define all random variables in the Bayesian network in Table 4.1. In Fig. 4.4, each vertex in the direct acyclic graph (DAG) represents a random variable, which has a probability distribution from experts' background knowledge. Each random variable is represented by two

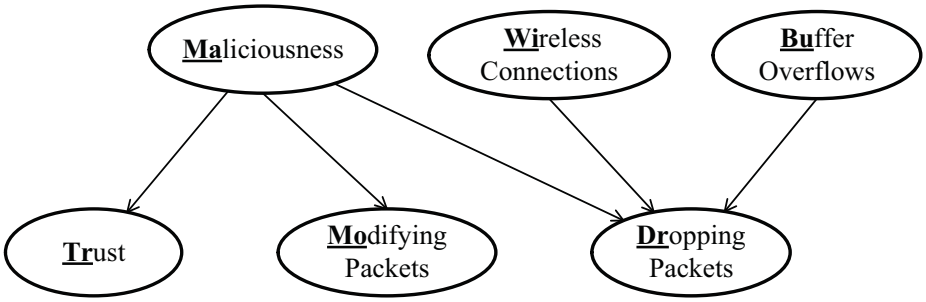

Figure 4.4: A Bayesian network for trust evaluation from self experience.

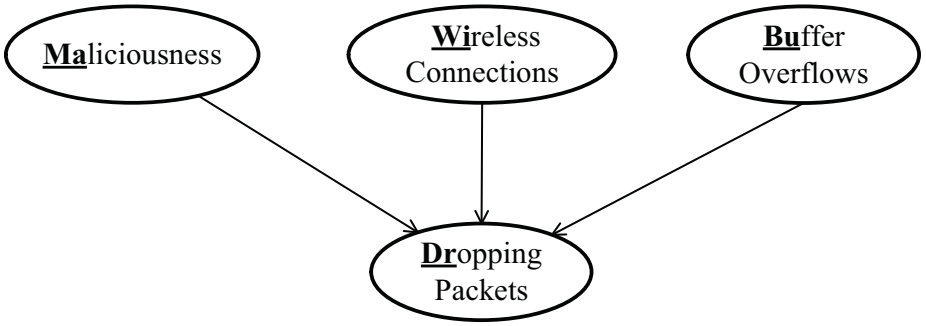

Figure 4.5: Converging connection in the Bayesian network.

bold capital letters in Fig. 4.4. Each vertex has an associated conditional probability distribution (CPD). For example, the CPD of vertex Dropping Packets is $p_{ij} = P(Dr|Ma, Wi, Bu)$. Vertices with no parents have CPDs given any events. Here, trust in the Bayesian network has three states in a discrete space: high, medium, and low. Generally, trust is measured by a real number between 0 and 1 (subjective probability), which is a continuous variable.

Then, we can calculate the joint probability distribution from the Bayesian network (Fig. 4.4).

$$\begin{aligned} P(\mathbf{X}) &= P(Ma)P(Wi)P(Bu) \\ &\quad P(Tr|Ma)P(Mo|Ma) \\ &\quad P(Dr|Ma, Wi, Bu), \end{aligned} \tag{4.3}$$

where $\mathbf{X} = \{Ma, Wi, Bu, Mo, Dr, Tr\}$. The trust value can be obtained by:

$$\begin{aligned} P(Tr) &= \sum_{Ma}\sum_{Wi}\sum_{Bu}\sum_{Mo}\sum_{Dr} P(Ma)P(Wi)P(Bu) \\ &\quad P(Mo|Ma)P(Dr|Ma,Wi,Bu) \\ &\quad P(Tr|Ma) \\ &= \sum_{Ma} P(Ma) \sum_{Wi} P(Wi) \sum_{Bu} P(Bu) \\ &\quad \sum_{Mo} P(Mo|Ma) \sum_{Dr} P(Dr|Ma,Wi,Bu) \\ &\quad P(Tr|Ma) \\ &= \sum_{Ma} P(Ma)P(Tr|Ma). \end{aligned} \tag{4.4}$$

Based on the Bayesian network, we can learn that how the trust of a node is affected by maliciousness with other factors. Therefore, causal reasoning in the Bayesian network [113] can be a good tool to calculate the trust of a node. At the beginning, we have no information or evidence about variable Tr, so $P(Tr)$ is calculated by default conditional probabilities. If new evidence that the observed node is malicious is found, then $P(Tr|Ma)$ becomes lower than the initial value. However, if the wireless connection is not good at the time, then $P(Tr|Ma, Wi)$ will increase to a higher value. Another reasoning named intercausal reasoning in the Bayesian network [113] can affect the prediction of maliciousness of an observed node. From background knowledge (if there is no background knowledge, usually, $P(Ma) = 0.5$), a node may have $P(Ma)$ with a lower or higher value. If the new evidence, such as dropping packets, is found, then $P(Ma|Dr)$ will increase. Nevertheless, if evidence of bad wireless connections is collected, then $P(Ma|Dr, Wi)$ will decrease. This formation of the Bayesian network (Fig. 4.5) is also defined as a converging connection [109]. In this situation, firstly, variable Ma and variable Wi are independent, also called d-separated in Bayesian networks. Then, the certainty of parents (maliciousness, buffer,

and wireless connections) may be transmitted if the child (dropping packets) can obtain information, which is also called hard evidence. When the vertex of dropping packets is instantiated (received evidence), the maliciousness and wireless connection vertices are d-connected [109]. Therefore, the certainty of wireless connection can affect the certainty of maliciousness. Even if the trust is identical, a node may be less malicious than its counterpart. In other words, if we know that the current state of wireless connection is unreliable, we would consider that the reason of dropping packets is more for unreliable wireless connection, than maliciousness. We assume that new observation $e = \{Wi = unreliable\}$, we then recalculate the trust value with the new observation following the Bayesian rule.

$$P(Tr|Dr = yes, e) = \frac{P(Tr, Dr = yes|e)}{P(Dr = yes|e)}. \tag{4.5}$$

Therefore, $P(Tr, Dr = yes|e)$ can be calculated by marginalizing the variables Ma, Mo, and Bu from $P(Tr, Ma, Bu, Mo, Dr = yes|e)$.

$$\begin{aligned} P(Tr, Dr = yes|e) &= \sum_{Ma}\sum_{Mo}\sum_{Bu} P(Tr|Ma) \\ &\quad P(Bu)P(Mo|Ma) \\ &\quad P(Dr = yes|Ma, Bu, e) \\ &= \sum_{Ma} P(Tr|Ma) \sum_{Bu} P(Bu) \\ &\quad P(Dr = yes|Ma, Bu, e) \\ &\quad \sum_{Mo} P(Mo|Ma) \\ &= \sum_{Ma} P(Tr|Ma) \\ &\quad P(Dr = yes|Ma, e). \end{aligned} \tag{4.6}$$

4.4 Simulation Results and Discussions

In this section, we present the effectiveness of the proposed scheme under packets dropping and modification attacks. First, we depict our experiment scenarios with pre-defined parameters. Next, we demonstrate the throughput and end-to-end delay of the proposed trust scheme based on a routing case study. Then, we compare our scheme and an existing scheme [114] w.r.t false alarm probability with an intrusion detection case study. Finally, we test the proposed scheme through a dynamic trust changing in the malicious environment.

4.4.1 Environment Settings

In our simulations, nodes are randomly placed in a space, area of which is from $800 \times 800\ m^2$ to $1300 \times 1300\ m^2$. The number of nodes is 5 to 30. Each node follows a random walk mobile model, where the velocity is between 0 m/s and 10 m/s. The transmission range of each node is 300 m. The data rate is $2M/s$. There is a source node that continuously send packets to a destination node in the network. The packet size is 512 bytes.

4.4.2 Performance Improvement

Two standard test criteria [101], throughput and average end-to-end delay, are used in our experiments to compare the proposed and existing schemes [114]. In Fig. 4.6, as the number of nodes in the MANETs increases, the throughput of both scheme declines. However, the proposed scheme has a better performance than the existing one because the trust values of malicious nodes in the proposed scheme are more accurate than its counterpart. As a result, the chance of successful data transmission between the MANET nodes is higher. Fig. 4.7 shows the proposed scheme has less

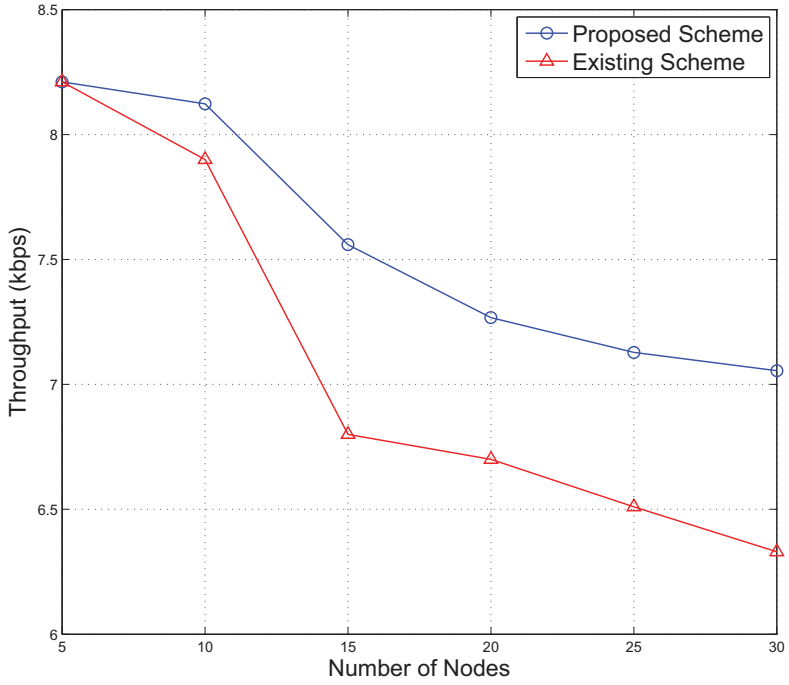

Figure 4.6: Throughput with different number of nodes.

end-to-end delay compared with the existing one. This is because a node that has a temporal poor wireless connection will be differentiated from the malicious one in the proposed scheme. Therefore, the chance of establishment of shorter paths between nodes is higher, which leads to lower average end-to-end delay. Due to the inference procedure in the Bayesian network model, the cost of computation is introduced during the trust evaluation. However, because the number of variable nodes in our Bayesian network is small, the added computation cost is negligible.

4.4.3 Malicious Nodes Detection with False Alarm Probabilities

The important function of a trust-based scheme is to detect the malicious nodes in MANETs with low false alarm probability. We compare the false alarm probabilities

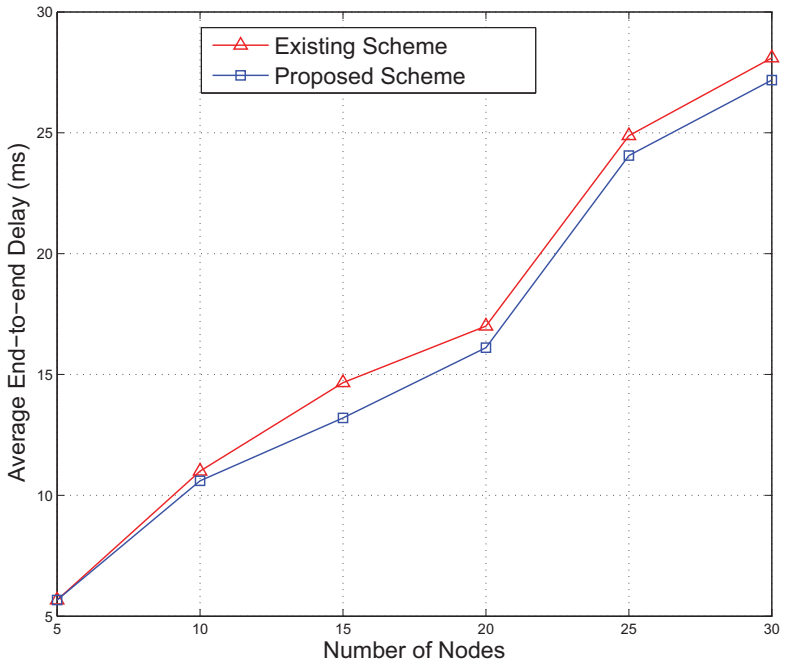

Figure 4.7: Average end-to-end delay with different number of nodes.

in two schemes. Trust values of a node with malicious intention in the MANET can be improved by the Bayesian network model, which accommodates causal relationships. In Fig. 4.8, as the threshold of trust value increases, the false alarm probability of the existing scheme grows up quickly. This is because of the nodes that have poor wireless connections are mistaken as malicious nodes. The false alarm probability of our scheme is very low because the accurate trust evaluation based on the Bayesian network model can differentiate maliciousness.

4.5 Chapter Summary

In order to utilize trust-based schemes for protection of MANETs, we need a more intelligent scheme to judge the intention of a node in MANETs. The simple assumption that all packets dropping behaviors caused by maliciousness is not realistic in many

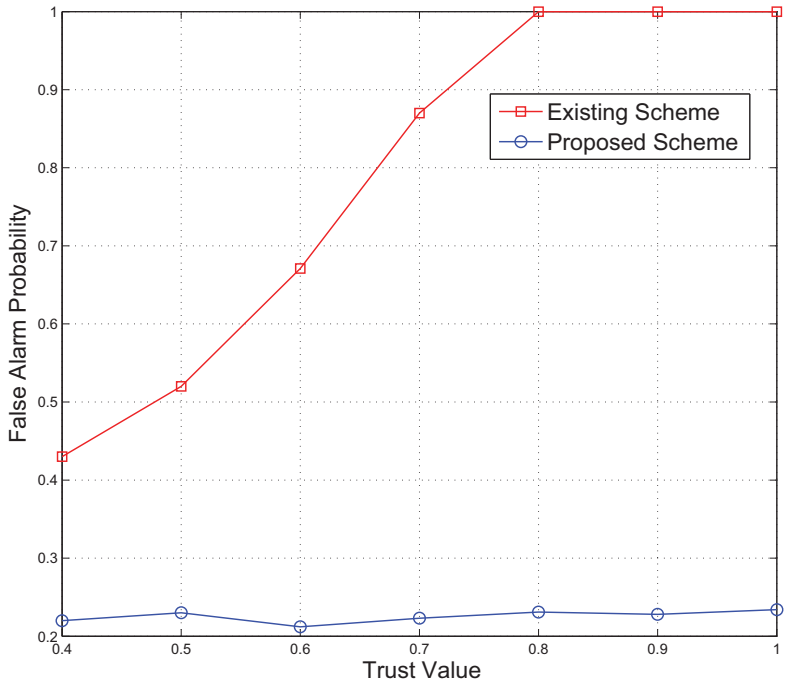

Figure 4.8: False alarm probability vs trust value.

circumstances. Therefore, we propose a trust-based scheme that utilizes Bayesian networks, which has advantages in causal reasoning with probability and graph theories. Depending on causal relationships in the Bayesian network, our scheme can obtain a more accurate trust value by differentiating malicious behaviors. As a result, the throughput performance of MANETs with the consideration of a variety of causes for packets dropping can be improved and the false alarm probability of the proposed scheme is lower.

Chapter 5

Trust Management in CR-MANETs

5.1 Introduction

Recently, cognitive radio (CR) has become a promising technology to deal with the spectrum shortage problem [115]. CR allows unlicensed (secondary) users to operate in the spectrum bands owned by licensed (primary) users. Since secondary users (SUs) are considered as lower priority, a basic requirement for SUs in CR networks is to avoid the interference to primary users (PUs) in their vicinity. In addition, PUs have no requirement to change their existing infrastructure to accommodate SUs. Consequently, SUs should have the capability of detecting the presence of PUs through spectrum sensing, and adaptively choosing transmission parameters according to sensing outcomes, which improves cognitive radio system performance and avoids interfering with PUs [115, 116].

CR technology has been applied to mobile ad hoc networks (MANETs), which enable wireless devices to dynamically establish networks without necessarily using a fixed infrastructure [117, 118]. CR technology will have significant impacts on the performance of MANETs. Certainly, issues in non-cognitive MANETs in general are still of interest in the CR paradigm. However, some distinct characteristics of CRs

introduce new non-trivial challenges to CR-MANETs.

One of the major challenges in CR-MANETs is *security* due to the involvement of intelligent nodes with self adaptation/context awareness capabilities in CR-MANETs. Particularly, a compromised node can take advantage of the intelligent cognition mechanisms in CR-MANETs to misbehave in a malicious manner. Therefore, in addition to the vulnerabilities and threats of traditional MANETs, the involvement of intelligence in CR-MANETs presents new security challenges.

In CR-MANETs, there are two main processes: *spectrum sensing* and *data transmission* [119, 120]. In the spectrum sensing process, mobile nodes detect the frequency bands that are not occupied by PUs; In the data transmission process, data packets are transmitted using the detected bands with a routing protocol. Both spectrum sensing and data transmission suffer many potential attacks in CR-MANETs, such as incumbent emulation (IE) attack and spectrum sensing data falsification (SSDF) attack [121] in spectrum sensing, and packet dropping/modification attacks in data transmission. In an IE attack, an attacker can mimic a false signal of the PU in order to disturb the sensing procedure. In an SSDF attack, an attacker can disturb the SUs' sensing results by disseminating fault sensing results deliberately in order to result in a wrong decision of the presence of PUs. A packet dropping attack is also called as a black hole attack, which is a type of denial-of-service attacks [25]. Modification of packets may have a significant impact on a topology map [26].

Although some excellent works have been done to address spectrum sensing security and data transmission security in CR-MANETs, these two important areas have traditionally been addressed separately in the literature. In this chapter, we propose to use a common framework to study *trust* management so as to enhance security for both spectrum sensing and data transmission processes in CR-MANETs. The motivations behind our work are based on the following observations.

- In previous works, it is generally assumed that a spectrum-sensing attacker will only attack the spectrum sensing process [17], and a data-transmission attacker will only attack the data transmission process [114]. However, it is highly possible for an intelligent attacker to attack both processes in CR-MANETs. Thus, the information to defense one process may be useful to defense another one.

- Both spectrum sensing and data transmission processes have significant impacts on the security of CR-MANETs. Considering these two processes jointly will be helpful to improve the performance of both processes.

- Recent works [122, 123] in the MANETs research areas have shown that trust-based approaches can be very effective in enhancing the security performance of wireless networks.

- Research works [61, 62] in spectrum sensing for CR have demonstrated that cooperative spectrum sensing can improve the performance of PUs detection but introduce the vast vulnerabilities in the security aspect.

To the best of our knowledge, the design of trust-based security schemes for both spectrum sensing and data transmission has not been considered in previous works.

The remainder of this chapter is organized as follows. Section 5.2 depicts the network model, the spectrum sensing model, the attack model, and the trust model. Section 5.3 describes a unified trust management scheme against JSSDT attacks. Section 5.4 explains the weighted consensus-based algorithm with trust. Section 5.5 describes the trust scheme for data transmission. The performance and effectiveness of our scheme are evaluated and discussed in Section 5.6. Finally, we conclude the work in Section 5.7.

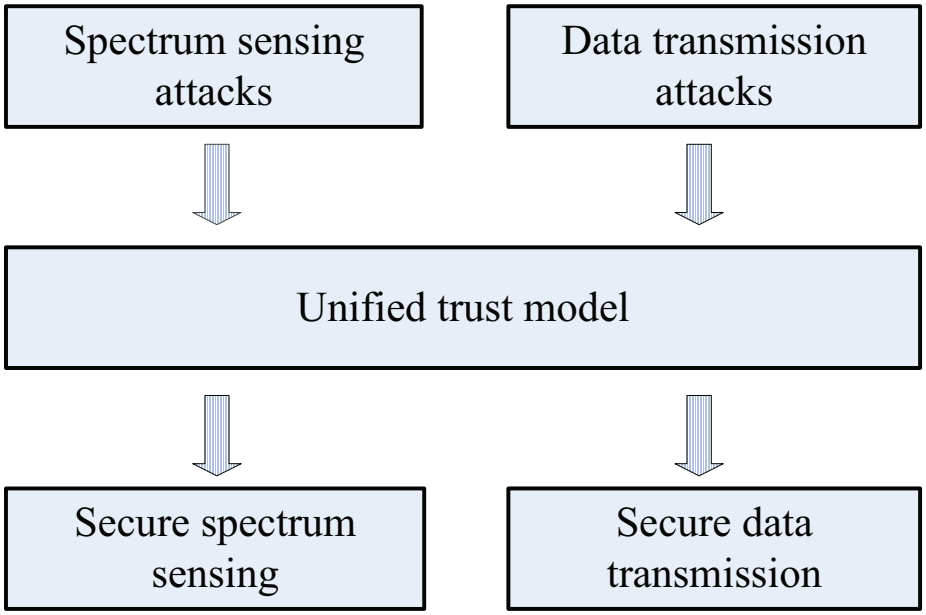

Figure 5.1: The framework of the proposed security schemes.

5.2 System Model

In this section, we present the network model firstly. Then we explain the spectrum sensing model used in this part. Finally, the attack model and trust model are described.

5.2.1 Network Model

CR as a promising technology can be applied in a variety of networks. Due to the distinguished characteristics of CR, networks with CR can be comprised of two parts: a PU network and an SU network. Both of them can form different network types, such as, centralized infrastructure networks or distributed ad hoc networks [124]. In this part, we consider a single PU in the network. Meanwhile, SUs in the network form a mobile ad hoc network [117], as shown in Fig. 5.2. There are two important tasks in each SU: spectrum sensing and data transmission. For spectrum sensing, SUs can independently detect the presence of a PU and report the sensing results to

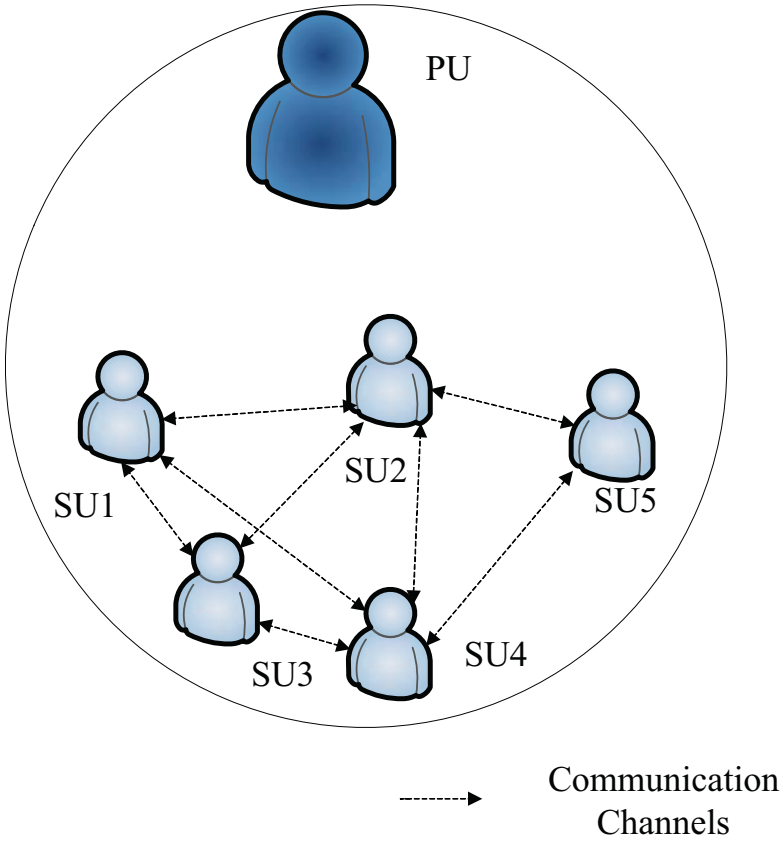

Figure 5.2: A CR-MANET with distributed cooperative spectrum sensing.

their neighbors [124]. If the PU is inactive, SUs can transmit data in the mobile ad hoc network using the spectrum bands owned by the PU.

5.2.2 Spectrum Sensing Model

The energy detection spectrum sensing method [125] is applied. SUs can detect the energy statistics of a PU with a hypothesis test. The hypothesis H_0 means that a PU is absent, otherwise the hypothesis H_1 implies that a PU is present. Following the

assumption in [61], the signal model of input is shown:

$$s(t) = \begin{cases} n(t), & H_0 \\ h * p(t) + n(t), & H_1 \end{cases} \tag{5.1}$$

where $s(t)$ represents the SU's received signal, $n(t)$ is the additive white Gaussian noise, h is the amplitude gain of the channel and $p(t)$ stands for the signal transmitted by PU. The output of energy detection of an SU has a probability distribution [17]:

$$Y = \begin{cases} \chi^2_{2\tau W}, & H_0 \\ \chi^2_{2\tau W-2} + Y_{exp}, & H_1 \end{cases} \tag{5.2}$$

where τW is the time-bandwidth product; $\overline{\gamma}$ is the average SNR; $\chi^2_{2\tau W}$ is a central chi-square distribution with $2\tau W$ degrees of freedom; Y_{exp} is an exponential distribution with parameter $2(\overline{\gamma}+1)$. After energy detection, an SU can obtain the estimate of the PU energy level, $Y \in \mathbb{R}^+$.

5.2.3 Attack Model

Due to the characteristics of CR-MANETs, there are two basic time slots, spectrum sensing and data transmission, in every periodic frame [119]. SSDF attack [121] is a serious security issue in cognitive radio networks. In SSDF, malicious SUs can report fake spectrum sensing results to its neighbors in order to interrupt the correct collaborative spectrum sensing procedure. Meanwhile, traditional attacks (e.g., packet dropping) during the data transmission process also significantly affect the performance of CR-MANETs. Based on these basic attack models, a new dynamic attack model, named *joint dynamic spectrum sensing and data transmission attack*, can be

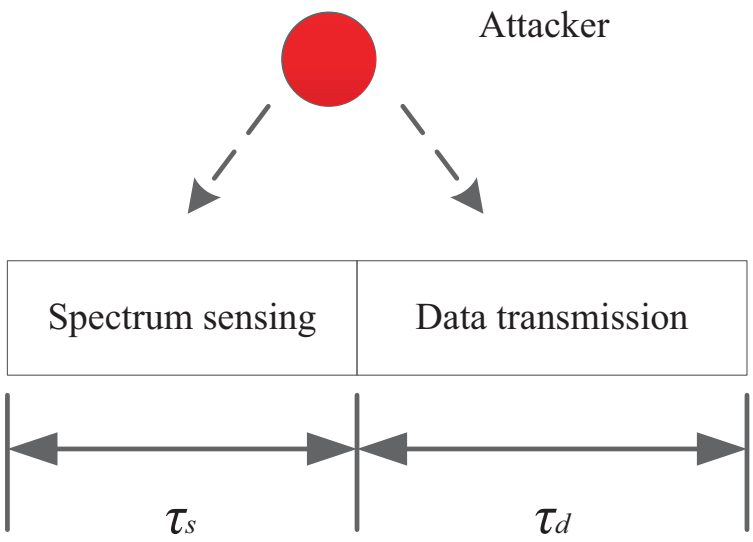

Figure 5.3: Joint spectrum sensing and data transmission attack (τ_s: spectrum sensing slot; τ_d: data transmission slot).

adopted by malicious SUs, as shown in Fig. 5.3. This attack model is a type of internal attacks. Compared to external attacks, internal attacks are difficult to defend effectively by authentication mechanisms. In this attack model, malicious SUs can do SSDF attacks in a spectrum sensing slot and packet dropping attacks in a data transmission slot.

Current secure spectrum sensing algorithms commonly assume that an attacker only adopts one fixed attack strategy all the time. If the attacker performs this new attack, then the performance of CR-MANETs will deteriorate. In order to detect this kind of malicious attackers, a unified trust management security scheme is presented in Section 5.3.

5.2.4 Trust Model

Trust is introduced in the field of network security as a mechanism to detect and defend malicious attacks. Trust is a complicated concept and has a variety of definitions

in different disciplines. In cognitive radio networks, trust also plays an important role in thwarting hostile attacks [124]. We adopt the definition of trust mainly from sociology and psychology. Trust is defined as degrees of belief that a network node can perform a duty as expected [4]. Due to the subjectivity of trust, trust can be varied greatly from node to node. Here trust is quantified by Bayesian probability, denoted as $T \in [0, 1]$.

Trust can be formed from two perspectives: direct observations and indirect observations (or recommendations) [4, 60]. Direct observations can help a trustor to evaluate the trust of a trustee by itself. Indirect observations are another important component for trust. If there are several network nodes that have interactions with the trustee, recommendations from these nodes can be treated as signification evidence for trust evaluation by the trustor. In order to obtain accurate trust of each node in the network, we combine these two parts together as follows.

$$T = \rho T^S + (1 - \rho) T^N, \tag{5.3}$$

where T^S is the trust value from direction interactions between a trustor and a trustee; T^N is the trust value from recommendations; $\rho \in [0, 1]$, is a weight used to represent the importance of each part.

5.3 Unified Trust Management for Both Spectrum Sensing and Data Transmission Processes

In this section, we present a unified trust management scheme to protect both spectrum sensing and data transmission processes. Firstly, we introduce the framework of our scheme. Then we explain the basic idea and procedure of our scheme.

5.3.1 Structure of the Unified Trust Management Scheme

The main goal of the proposed security scheme is to protect both spectrum sensing and data transmission from attacks performed by smart adversaries in cognitive radio environments and to improve the performance of CR-MANETs. As mentioned in Subsection 5.2.3, a malicious attacker can interrupt the normal traffic in both spectrum sensing and data transmission slots. Based on recent advances in distributed consensus research and computational trust in multi-agent systems [14, 126], we present a unified trust management scheme in order to handle this new attack in CR-MANETs.

The structure of our proposed scheme is depicted in Fig. 5.4. The modules in this structure are explained as follows. The detection module consists of different approaches of spectrum sensing, e.g., energy detection. The observation module is in charge of collecting evidence about behaviors of neighbor SUs. The trust calculation and update module can utilize the evidence provided by the observation module to evaluate the trust of neighbors by a variety of methods, e.g., Bayesian inference. The trust repository stores the trust of neighbors and provides them to upper modules, such as consensus-based spectrum sensing and data transmission. The consensus-based spectrum sensing module can use trust as weights to fuse the results from detection. The data transmission module can use the trust to select reliable routing paths. Based on this framework, our scheme can effectively boost the performance of CR-MANETs with malicious SUs.

5.3.2 Procedure of the Unified Trust Management Scheme

The basic idea of our scheme is to use the trust obtained from observations as the weights of the distributed consensus algorithm so that the spectrum sensing reports from untrusted SUs can be marginalized. Meanwhile, the trust scheme can improve the performance of data transmission among SUs. The main procedure has two phases

described as follows:

- In the spectrum sensing phase, each SU performs a weighted-average consensus algorithm to calculate the sensing result. Because there is a trust value as the weight for each SU, which obtained from the data transmission phase, the sensing result will be dominated by the trusted SUs. After each distributed consensus-based spectrum sensing, each SU can recognize which one reports the sensing result that has the largest deviation [17]. The scheme will record this SU in a history log, which is used to evaluate trust in the data transmission phase.

- In the data transmission phase, we use the direct and indirect observations to evaluate the trust of each SU. A trust evaluation mechanism will be explained in detail in Section 5.5. Meanwhile, based on the history log obtained from the spectrum sensing phase, the SU with the largest deviation of the sensing result has the highest probability to misbehave during the data transmission phase. Utilizing the information from these two phases, the scheme can calculate the unified trust value for both of them.

In the next two sections, we will describe the weighted-average consensus algorithm and trust establishment in more detail.

5.4 Weighted Consensus-based Spectrum Sensing Scheme Based on Trust

In this section, we first introduce consensus notations. Then we describe the weighted-average consensus algorithm with trust.

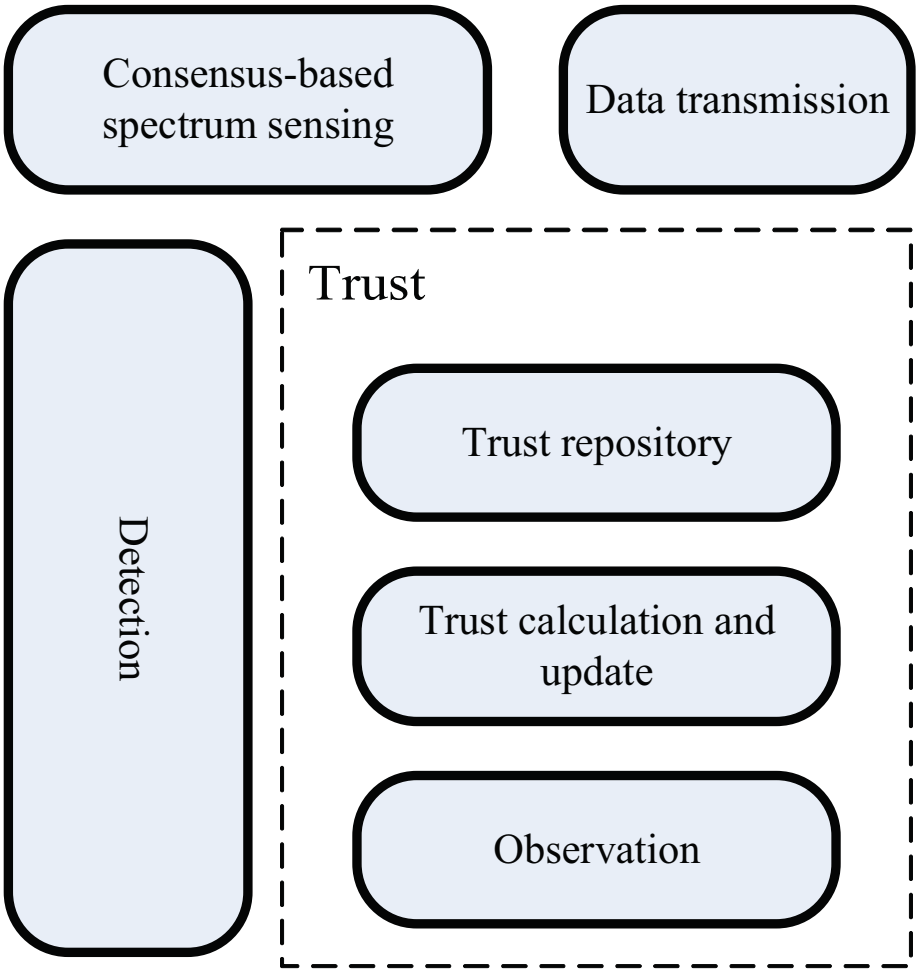

Figure 5.4: The structure of the unified trust management scheme.

5.4.1 Consensus Notations

In CR-MANETs, the network formed by SUs is presented by an undirected graph, which is denoted by $\boldsymbol{G} = (\mathcal{V}, \mathcal{E})$. $\mathcal{V}$ is a set of vertices in the graph. The set of edges in the graph is $\mathcal{E} = \{(i,j)|i,j \in \mathcal{V}\}$. We assume that if two SUs are in the radio range, they are connected by an edge in the graph. The neighbors of vertex i belong to a neighbor set $N(i) = \{j \in \mathcal{V}|i \neq j, \exists(i,j) \in \mathcal{E}\}$. The *degree* of a vertex i is defined as the number of edges connected to the vertex, denoted as $d(i)$. An undirect simple graph, $\boldsymbol{G} = (\mathcal{V}, \mathcal{E})$, can be represented by a matrix $\boldsymbol{A} = (a_{ij})_{n\times n}$, where

$$a_{ij} = \begin{cases} 1, & \text{if } j \in N(i) \\ 0, & \text{otherwise} \end{cases} \tag{5.4}$$

5.4.2 Weighted-average Consensus Algorithm

Performing distributed cooperative spectrum sensing in the normal environment, each SU is honest and cooperative and sends the sensing results of the PU energy correctly. With this assumption, the average-consensus algorithm can be executed very well [4]. However, in the malicious environment, an SU may send false results deliberately in order to disrupt the average-consensus algorithm. SUs that provide sensing data are trusted or not depending on trust evaluation. Using trust values as weights, the weighted-average consensus algorithm is a means to reduce the impact of false sensing data reported by malicious SUs.

In the weighted-average consensus [127, 128], we apply the trust value of each

neighbor SU as the weight. Considering the discrete time situation, the weighted-average consensus algorithm can be formulated as follows:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in N_i(k)} w_{ij}(x_j(k) - x_i(k)), \tag{5.5}$$

where $0 < \epsilon < (\max_i |N_i|)^{-1}$, w_{ij} is a weight for SU i to every its neighbor.

The states of SUs are updated by previous states. From (5.5), we can see that weighted-average consensus is an iterative procedure. Next, we explain how to use the weighted-average consensus algorithm to our scheme.

The proposed weighted-average consensus spectrum sensing scheme with trust is depicted in Algorithm 3. First, every SU detects the energy status of the PU with energy detection. After detection, every SU can exchange local estimated energy of the PU with its neighbors. The local result of an SU can be updated by (5.5) in iterations. Specifically, in each iteration, each SU can receive the energy values from its neighbors and then calculate the new local result with the old one and neighbor estimated values with weights. Finally, each SU delivers its new result to its neighbors when it finishes self calculation. The termination condition of iterations is that the difference between the new result of each SU and a common consensus value is less than or equal to a tolerant deviation. When the final consensus value is achieved, SUs can compare the value with a pre-defined threshold [61] to conclude a final distributed decision that whether or not the PU is present.

Here each weight of the neighbor SU is set to an real number [128], which can be defined as

$$w_{ij} = \frac{T_{ij}}{1 + \sum_{j \in N(i)} T_{ij}}. \tag{5.6}$$

When $k \to \infty$ in (5.5), $x_i(k) \to x^*$ [128]. Using Algorithm 3, the SU that has a

Algorithm 3 Weighted-average Consensus Spectrum Sensing with Trust

obtain the energy value of the PU by self with the energy detection method
set x to the energy value
set x^* to a final common consensus value
set ε to a tolerant deviation
set $k = 0$
while ($x - x^* > \varepsilon$) **do**
  collect energy values of the PU from neighbors
  set x to a new local value by (5.5)
  send x to neighbor SUs
  $k = k + 1$
end while
set λ to a pre-defined threshold
if ($x \geq \lambda$) **then**
  the final decision is that the PU is present
else
  the final decision is that the PU is absent
end if

higher trust value can affect the update result more. Therefore, trustful SUs will dominate the final consensus result and meanwhile the impact from malicious ones will be marginalized. At the end, the correct decision can be made in the hostile environment.

5.5 Secure Data Transmission Based on Trust

In this section, we describe the trust establishment procedure for secure data transmission. Firstly, we describe the trust obtained from direct observations. Then, the trust obtained from indirect observations is introduced. Finally, we present a trust based routing scheme for data transmission.

5.5.1 Trust from Direct Observations

We propose a modified Bayesian framework considering the mobility of SUs to evaluate the trust of SUs during the data transmission slot. In the Bayesian framework, the prior distribution is known and the posterior distribution is updated by evidence collection. Here, we use this framework to evaluate trust values of an observed SU. We assume that each SU performs maliciously with with two types of attacks: dropping packets attack and modifying packets attack. In order to calculate trust values of an observed SU, we assume that if an observed node is malicious then it will drop or modify packets from other SUs, which should be forward correctly. In this context, we treat the trust value of an observed node as a probability, $\theta \in [0, 1]$, of forwarding packets correctly. θ can be modeled as a value of a continuous random variable Θ and the prior probability density function is f_Θ. Each packet is dropped or modified independently by the malicious SU. Following the standard Bayesian approach [84], we can obtain the posterior probability density function of the random variable Θ,

$$f_{\Theta|E}(\theta|e) = \frac{p_{E|\Theta}(e|\theta) f_\Theta(\theta)}{\int p_{E|\Theta}(e|\theta') f_\Theta(\theta') \, \mathrm{d}\theta'}, \tag{5.7}$$

e is the evidence obtained by an observer. The formulation can be simplified as

$$f_{\Theta|E}(\theta|e) = c p_{E|\Theta}(e|\theta) f_\Theta(\theta), \tag{5.8}$$

where c is a normalization constant. In our context, the likelihood function, $p_{E|\Theta}(e|\theta)$, can be modeled as a binomial distribution, in which n is the total packets received by the observed node and L is the number of packets forwarded correctly. Thus, the formula of the likelihood function is

$$p_{E|\Theta}(e|\theta) = p_{L|\Theta}(l|\theta) = \binom{n}{l} \theta^l (1-\theta)^{n-l}. \tag{5.9}$$

We assume that the prior probability density function is a beta density function

$$f_{\Theta}(\theta) = \frac{\theta^{\alpha-1}(1-\theta)^{\beta-1}}{\int_0^1 \theta^{\alpha-1}(1-\theta)^{\beta-1}\,\mathrm{d}\theta}, \tag{5.10}$$

where $0 \leq \theta \leq 1, \alpha > 0, \beta > 0$. The posterior probability density function can be obtained from (5.8), (5.9), and (5.10).

$$f_{\Theta|E}(\theta|e) = c' \frac{\theta^{l+\alpha-1}(1-\theta)^{n-l+\beta-1}}{\int_0^1 \theta^{\alpha-1}(1-\theta)^{\beta-1}\,\mathrm{d}\theta}, \tag{5.11}$$

where $c' = c\binom{n}{l}$. Here, the posterior probability density function is also a beta function. With the posterior function, we can obtain the estimate of θ, denoted as $\hat{\theta}$. We adopt the Least Mean Squares (LMS) estimator [84] to calculate the estimate of θ. Then,

$$T^S = \hat{\theta} = E[\Theta|L = l] = \frac{\alpha + l}{\alpha + \beta + n}. \tag{5.12}$$

Under the CR context, considering the mobility of SU, we exclude the packets dropping from the impact of PU's activities. The measurement of the mobility of SUs is conducted with a link-availability prediction model in [120]. In this model, we can obtain the available time interval, τ_a, of a link between two SUs,

$$\tau_a = \tau_p \times p(\tau_p), \tag{5.13}$$

where τ_p is the time of a link between two SUs can maintain; $p(\tau_p)$ is a probability that a link can be held during τ_p. From (5.12) and (5.13), we can improve the trust value:

$$T^S = \frac{\alpha + l}{\alpha + \beta + \frac{\tau_a}{\tau_d}(n - l) + l}, \tag{5.14}$$

where τ_d is a time slot of data transmission. If the available time period is larger than the data transmission slot, then we believe that the dropping packets are caused by maliciousness and the trust value is calculated by (5.12); otherwise, the dropping packets are caused by mobility during the unavailable time period of a link and the trust value is calculated by (5.14).

5.5.2 Trust from Indirect Observations

As another important component of trust, trust from indirect observations can facilitate an observer SU to evaluate trust values of an observed SU by collecting evidence from its neighbors that have interactions with the observed one. During the procedure of trust evaluation from neighbors' opinions or recommendations, there are two significant steps: collection and combination of information from SUs. For the information collection, each SU has the interaction with an observed SU can provide evidence to an observer SU from itself perspective. The evidence has different quality or reliability. Different SUs may have different opinions about the same observed SU. Even the same provider of evidence also perhaps has different opinions about the same observed SU. In other words, evidence collected by an observer SU is varied at the level of reliability. For the combination of recommendations, the observer SU needs to calculate a trust value through the evidence provided by other SUs independently. In these specific contexts, the Dempster-Shafer theory (DST), a mathematical theory of evidence [13], is a better choice to evaluate the trust from indirect observations than the major voting mechanism [70]. DST is developed initially by Dempster and improved and extended by Shafer, then prospers in artificial intelligence community,

especially in the field of expert systems [13]. There are two distinguished features in DST: a query of interested proposition via a related question and a combination rule of independent evidence [13]. In order to explain how to apply DST to trust evaluation from indirect observations, we need to introduce DST in brief.

In DST, a finite set that includes all possible states of a variable is defined as a *frame of discernment* [70], denoted as Ω. In Ω, all elements are mutually exclusive and exhaustive. The power set of Ω is defined as 2^{Ω}, which is comprised of all subsets of Ω, including $\emptyset$ and Ω self. Each element in the power set is called a focal set, R_i, in DST. There is a basic probability value for each focal set using a mapping function $m : 2^{\Omega} \longrightarrow [0, 1]$. The function m fulfils two axioms [13]:

$$m(\emptyset) = 0, \tag{5.15}$$

and

$$\sum_{R_i \subseteq \Omega} m(R_i) = 1. \tag{5.16}$$

Based on the definition of m, the belief function [13] is

$$bel(Z) = \sum_{R_i \subseteq Z} m(R_i). \tag{5.17}$$

and the plausibility function [13] is

$$pl(Z) = \sum_{R_i \cap Z \neq \emptyset} m(R_i). \tag{5.18}$$

The combination rule of two belief functions [13] is

$$bel(Z) \quad = \quad bel_1(Z) \oplus bel_2(Z)$$

$$= \frac{\sum_{i,j,R_i \bigcap R_j = Z} m_1(R_i) m_2(R_j)}{\sum_{i,j,R_i \bigcap R_j \neq \varnothing} m_1(R_i) m_2(R_j)}. \quad (5.19)$$

Then, we explain how to use DST in our scenario. A neighbor SU C that provides evidence about an observed SU to an observer, which is trustworthy or not. Thus $\Omega = \{trustworthy, malicious\}$ and $2^{\Omega} = \{\emptyset, \{trustworthy\}, \{malicious\}, \Omega\}$. If SU C believes that the observed SU is trustworthy, the belief functions of SU C about the observed SU can be deduced as:

$$\begin{aligned} m_C(R_1) &= T^S_{AC}, \\ m_C(R_2) &= 0, \\ m_C(\Omega) &= 1 - T^S_{AC}, \end{aligned} \quad (5.20)$$

where $R_1 = \{trustworthy\}$, $R_2 = \{malicious\}$, and T^S_{AC} is the trust value from the observer to SU C. Similarly, if SU C believes that the observed SU is malicious, the belief functions are:

$$\begin{aligned} m_C(R_1) &= 0, \\ m_C(R_2) &= T^S_{AC}, \\ m_C(\Omega) &= 1 - T^S_{AC} \end{aligned} \quad (5.21)$$

If there are several neighbor SUs, the combination rule is applied to belief functions. Then the trust value from indirect observations between SU A and B can be calculated by

$$T^N_{AB} = m_{C_1}(R_1) \oplus m_{C_2}(R_1) \ldots \oplus m_{C_n}(R_1), \quad (5.22)$$

where SU C_i, $1 \leq i \leq n$, is a neighbor SU between SU A and SU B.

5.5.3 Trust Based Routing Scheme for Data Transmission

The proposed trust model can be applied to a variety of routing algorithms. Here, in order to illustrate our scheme in CR-MANETs, we use Dijkstra algorithm, which is a link state routing algorithm. Following the definition of routing metric in [129], D_{AB} is defined as:

$$D_{AB} = \frac{d_{AB}}{T_{AB}}, \tag{5.23}$$

where D_{AB} is the routing metric between SU A and SU B; d_{AB} is the distance metric between SU A and SU B; T_{AB} is the trust value from SU A to SU B. For simplicity, we use hop count as the distance measure in our scenario. When T_{AB} approaches 0, the routing metric becomes infinite and can be excluded by Dijkstra algorithm. Based on routing metric calculation, Dijkstra algorithm can find the shortest trusted path between a source and a destination.

5.6 Simulation Results and Discussions

In this section, we show the effectiveness of the proposed scheme in CR-MANETs under joint dynamic spectrum sensing and data transmission attacks. We compare the false alarm probabilities and miss detection probabilities of the proposed scheme with those of an existing consensus-based cooperative spectrum sensing scheme [130], which removes the sensing data that has the maximum deviation during the consensus procedure. Finally, we compare the performance of data transmission under the attacks.

In our simulations, SUs are randomly placed in a square space with the area from 800×800 m^2 to 1200×1200 m^2. The number of SUs is between 5 and 30. Each SU follows a random walk mobility model with the velocity from 5 m/s to 30 m/s.

The transmission range of each SU is 300 m. During the spectrum sensing slot, each SU adopts the energy detection mechanism to sense the presence of a PU with an assumption that each SU performs spectrum sensing in a fading channel with Rayleigh distribution. During the data transmission time slot, the transmission rate is 2 Mb/s.

5.6.1 Defense against Joint Dynamic Spectrum Sensing and Data Transmission Attacks

In this simulation scenario, there are 1 PU and 11 SUs. The SUs perform the cooperative spectrum sensing procedure to detect the presence of the PU, and then decide whether or not data transmission can be executed. First, we present the results when SUs perform cooperative spectrum sensing without malicious attacks. The distributed consensus-based spectrum sensing with security mechanisms [130] (Fig. 5.5) and the proposed scheme (Fig. 5.6) are compared. From Figs. 5.5 and 5.6, we can observe that SUs can finally come to a consensus, and make a decision that the PU is absent. The existing consensus-based scheme reaches the consensus after 60 steps. By contrast, the proposed scheme has fewer steps to achieve the consensus, which shows the faster convergence rate of the proposed scheme compared with the exiting one. This is because the existing consensus-based scheme excludes an SU that reports detection statistics with the maximum deviation from the local mean during each consensus calculation. Since the SU with the maximum deviation does not necessarily means that it is a malicious SU, the proposed scheme shows superior performance in terms of the convergence rate compared with the existing consensus-based scheme.

In the malicious environment, an SU launches joint dynamic spectrum sensing and data transmission attacks (i.e., sending falsified sensing reports and dropping packets). Here, the malicious SU attacks both spectrum sensing and data transmission processes. In order to avoid the detection others, the malicious SU generates wrong

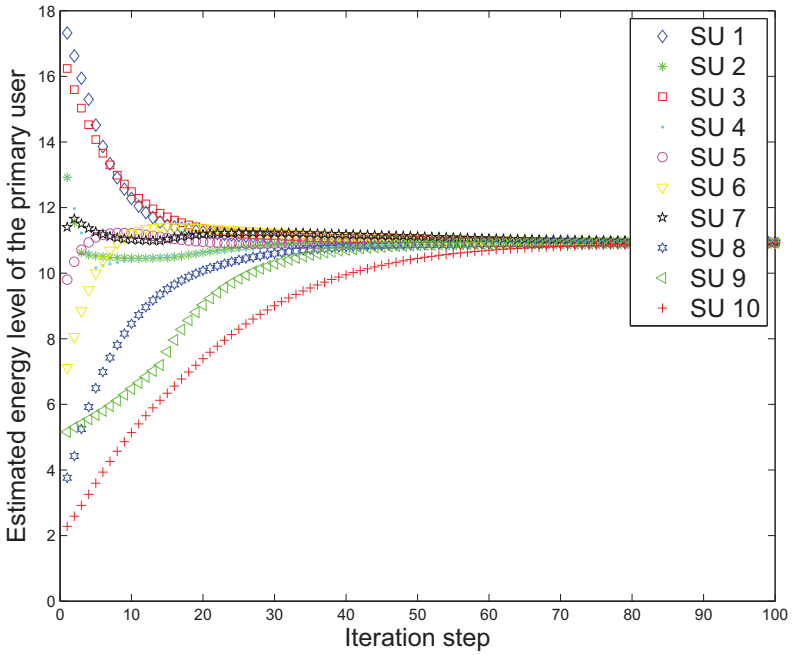

Figure 5.5: The existing consensus-based scheme without attacks.

sensing data that does not have the largest deviation. Fig. 5.7 shows that the existing consensus-based scheme cannot exclude the malicious SU when it adopts this intelligent strategy. Consequently, a wrong decision is made that the PU is present. By contrast, in Fig. 5.8, the proposed scheme lowers the weight of the malicious SU and facilitates the consensus procedure. As a result, the proposed scheme can make a correct decision that the PU is absent.

5.6.2 Performance Improvement with False Alarm Probabilities and Miss Detection Probabilities

The performance of our scheme is further evaluated by two metrics: *false alarm probability*, denoted by P_f and *miss detection probability*, denoted by P_m [17, 125]. Similar to intrusion detection systems, the tradeoff between P_f and P_m is an important

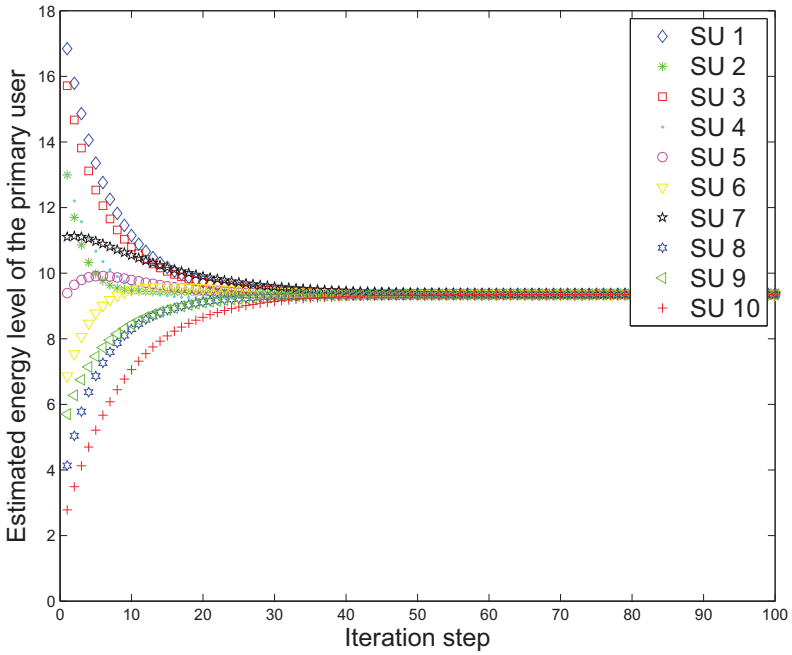

Figure 5.6: Our proposed scheme without attacks.

issue in dynamic spectrum sensing [17, 125].

We compare the performance of the proposed scheme with that of the existing consensus-based scheme. The pre-defined threshold in our simulations is set to $\lambda = 11.4dB$. The first case is that one compromised SU performs the joint dynamic spectrum sensing and data transmission attacks. In the second case, there is no attack. Fig. 5.9 shows that the proposed scheme outperforms the existing consensus-based scheme in terms of the false alarm probabilities. The existing consensus-based scheme suffers the attacks and causes the higher false alarm probabilities. Under the no attack condition, the existing consensus-based scheme has higher false alarm probabilities, because it always excludes an SU with maximum deviation of sensing data even if the SU is not malicious. In Fig. 5.10, the proposed scheme has lower miss-detection probabilities. This is because the proposed scheme can degrade the weight of the malicious SU without filtering out the SU with the maximum deviation.

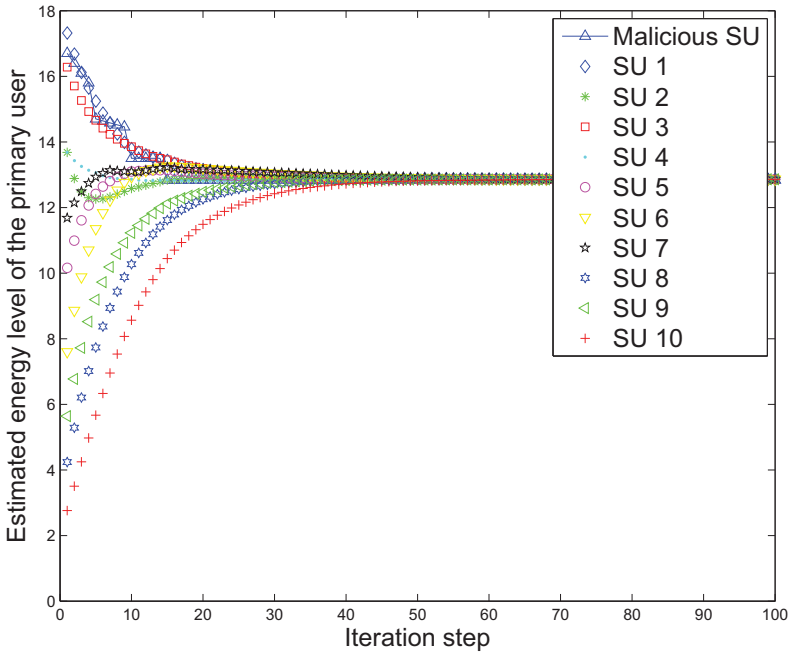

Figure 5.7: The existing consensus-based scheme with joint dynamic spectrum sensing and data transmission attacks.

It is reasonable that the existing consensus-based scheme and proposed scheme have similar miss detection probabilities under the case with no attack.

5.6.3 Performance Improvement for Data Transmission

Successful data transmission is an important aspect in CR-MANETs. We consider two criteria for the performance of data transmission: throughput and average end-to-end delay. We compare the proposed scheme, the existing consensus-based scheme [130], and the existing trust-based scheme [114], under joint dynamic spectrum sensing and data transmission attacks. In the existing consensus-based scheme [130], each SU adopts the spectrum sensing scheme, as explained at the beginning of this section. However, there is no protection during data transmission. In the existing trust-based scheme [114], each SU performs data transmission based on the trust value

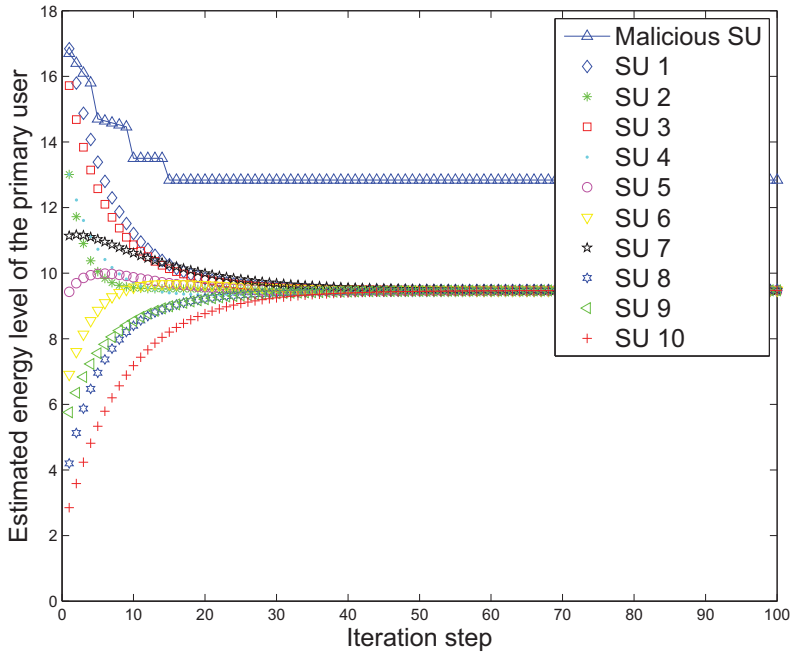

Figure 5.8: Proposed scheme with joint dynamic spectrum sensing and data transmission attacks.

derived from the data transmission process only, without considering the attacks in the spectrum sensing process. Fig. 5.11 shows that the proposed scheme has a higher throughput than the existing consensus-based and the trust-based schemes. This is because the proposed scheme provides a trusted path for SUs with data transmission, considering the attacks in both spectrum sensing and data transmission processes. For the existing trust-based scheme, the malicious SU's activities seriously affect the throughput of data transmission. In general, the performance of these schemes is affected by the mobility of SUs. As the maximum velocity increases, the throughput declines. In addition, Fig. 5.12 shows that the proposed scheme has a larger average end-to-end delay than the existing counterparts. The reason is that a trusted path may be longer than the shortest one in terms of hop count. Nevertheless, the increase of average end-to-end delay is trivial in the proposed scheme.

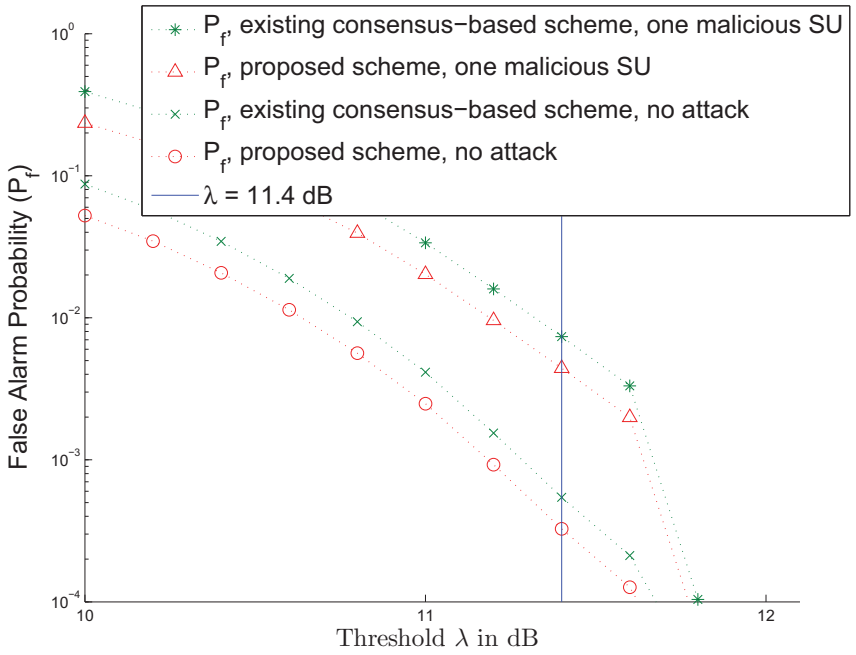

Figure 5.9: False alarm probability comparison between the existing consensus-based scheme and the proposed scheme.

5.7 Chapter Summary

Cognitive radio technology provides a venue to boost idle licensed spectrum utilization. Security in spectrum sensing and data transmission is a significant issue in cognitive radio mobile ad hoc networks (CR-MANETs). We introduced a new attack, named joint spectrum sensing and data transmission (JSSDT) attack, which can dramatically disrupt the normal functions of CR-MANETs. Using recent advances in the theory of uncertain reasoning, we developed a unified trust management scheme with both direct observation and indirect observation. Based on the unified trust model, we presented schemes to protect both spectrum sensing and data transmission processes. Simulation results demonstrated the effectiveness of the proposed schemes in CR-MANETs.

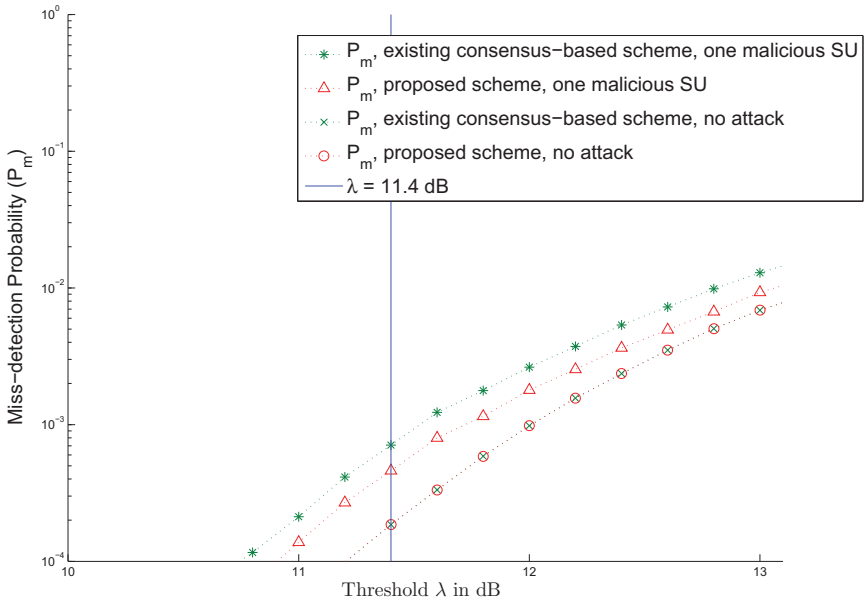

Figure 5.10: Miss-detection probability comparison between the existing consensus-based scheme and the proposed scheme.

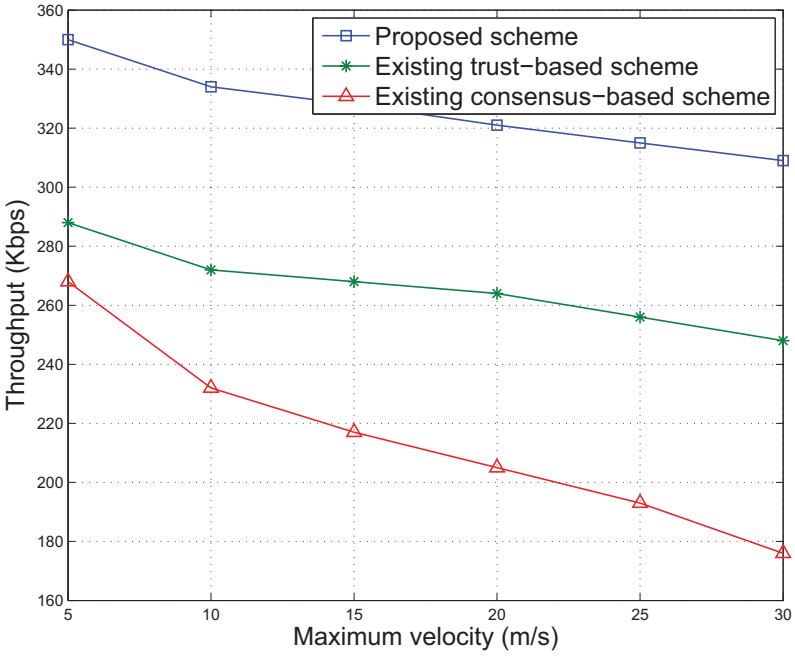

Figure 5.11: Throughput versus maximum velocity.

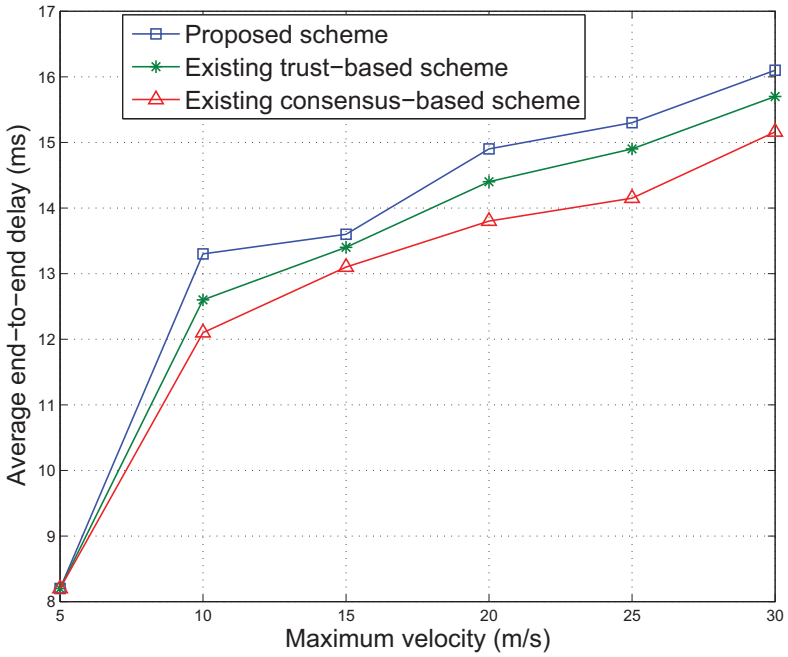

Figure 5.12: Average end-to-end delay versus maximum velocity.

Chapter 6

Securing CR-VANETs with Trusted Cloud Computing

6.1 Introduction

Recently, there is a phenomenal burst of interest in connected vehicles (CVs). CV systems use connectivity (via advanced wireless communications) to enable vehicles, smart roadway infrastructure (SRI) and personal mobile devices to exchange information with each other, and to provide road users with both safety and mobility advisories, warnings and alerts [131]. Vehicular Ad hoc NETworks (VANETs) as the basic infrastructure can facilitate applications and services of CVs [132]. Safety and entertainment are the main topics and incentives of CVs, which are drawing great interest from both academia and industry. To achieve these two primary goals, several challenges in VANETs need to be solved. The first one is the *limited resources*, such as radio spectrum resources, computation and storage resources. The second one is the *latency requirement* from driving applications and services, which is stricter than traditional network applications' requirements. In addition, *security* is also very critical for VANETS.

For the limited radio spectrum issue, a promising solution is *cognitive radio* [115,

117], which has already extended to VANETs environments [115]. Generally, CR technology can help secondary users (SUs) that have no pre-defined spectrum for wireless communications to utilize the primary users (PUs)' licensed spectrum. The condition is that the SUs should not interrupt the PUs' normal communications. In other words, SUs should have the ability to detect the presence of PU and concede the licensed spectrum for the PU. In addition, PUs have no requirement to change their existing infrastructure to accommodate SUs [46, 82, 116, 117, 130, 133–137]. In VANETs, CR technology can be used to mitigate the spectrum limitation issue.

For the issue of limited computation and storage resources, cloud computing in VANETs can leverage the limited capability of a specific vehicle by using the idle computing units and storage space from other vehicles and roadside units (RSUs) [39]. Cloud computing for VANETs can basically provide three types of services for the vehicle tenant: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) [39]. For SaaS, the vehicle can perform the applications or services, which are already in the cloud computing service, e.g., weather forecasting. For PaaS, the vehicle can perform its applications on the platform, such as operating system, provided by cloud services. For IaaS, the vehicle can request a larger space on the cloud to store the entertainment videos temporarily.

The low latency requirement is extremely important in CR-VANETs with cloud computing due to the high dynamic characteristics in the driving scenarios [44]. This makes the traditional and powerful cloud on the Internet hard to satisfy the applications and services in CR-VANETs. The vehicular cloud, which is comprised of vehicles and RSUs autonomously, is an attractive and possible alternative. Compared to the traditional cloud, it can have lower latency [138].

Last but not least, security in the VANETs is the key to make any service or

application successful in the safety driving condition. Security permeates every corner in CR-VANETs, from spectrum sensing to networking, from software to cloud computing. In spectrum sensing, the sensing data falsification attack (SSDF) [48] is a notable attack. In networking, the packet dropping attack or black hole attack is a big threat [19]. These security issues need to be carefully addressed.

Although several research works have been done to address security issues in CR-VANETs and cloud computing in VANETs, securing CR-VANETs with trusted light-weighted cloud computing has not been studied yet. In this chapter, we propose a joint RSU and vehicle-based light-weighted cloud for CR-VANETs. Based on this cloud computing model, we propose a new service named Spectrum Sensing as a Service (SSaaS), which can perform a cooperative spectrum sensing in CR-VANETs with cloud computing assistance to secure the spectrum sensing procedure. As a result, a reliable service can be obtained in CR-VANETs. Simulation results show that the cloud computing in CR-VANETs can effectively reduce latency and improve the security of CR-VANETs.

The remainder of this chapter is outlined as follows. We describe the CR-VANETs in Section 6.2.1. The cloud computing model in VANETs is introduced in Section 6.2.2. Then we explain the security issues in CR-VANETs in Section 6.2.3. Next, the proposed architecture is illustrated in Section 6.3 The simulation results are showed and discussed in Section 6.4. Finally, we give the conclusion of the work in Section 6.5.

6.2 Security Issues in Cognitive Radio Vehicular Ad Hoc Networks with Cloud Computing

In this section, we first introduce CR-VANETs, followed by cloud computing in CR-VANETs. Then, the security issues are discussed.

6.2.1 Cognitive Radio Vehicular Ad Hoc Networks

CR-VANETs are proposed to solve the issue of spectrum shortage in vehicular networks. Vehicles equipped with CR technology can communicate with each other through the licensed spectrums owned by the PU. These vehicles form a network, which is the secondary network. Cooperative spectrum sensing can be adopted in CR-VANETs due to its dynamic and mobile nature. Each vehicle detects the presence of the PU independently. Energy detection of spectrum sensing can be used as the detection method of each vehicle due to its simplicity. In this chapter, we consider the RSUs as fixed units, which can also participate the cooperative spectrum sensing process to improve the accuracy of the sensing results. Fig.6.1 shows a CR-VANET that consists of several vehicles and a RSU. SUs (including vehicles and RSU) in this network can perform cooperative spectrum sensing in order to detect the status (i.e., presence or absence) of the PU.

6.2.2 Cloud Computing in VANETs

Cloud computing in VANETs can extend the computation ability and storage space of each vehicle. There are three types of services that cloud computing in VANETs can provide: software as a service, infrastructure as a service, and platform as a service. Due to the mobility and constraints of cloud computing in VANETs, the cloud is typically categorized by three levels hierarchically: Internet-based cloud, RSU-based

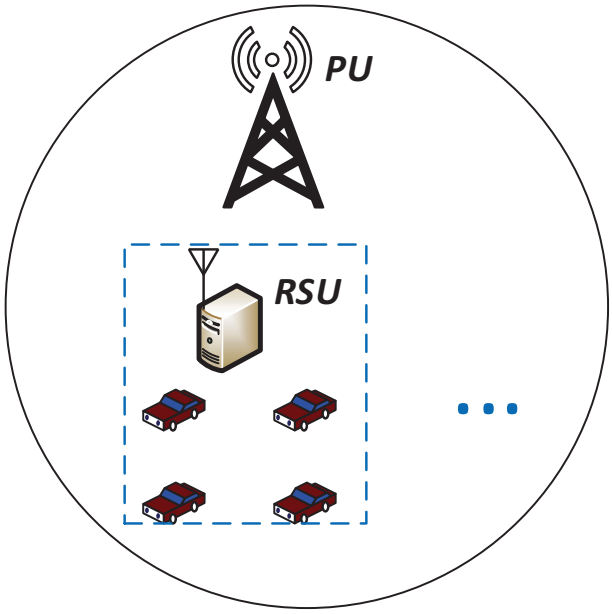

Figure 6.1: A cognitive radio vehicular ad hoc network with RSU.

cloud, and vehicle-based cloud. Internet-based cloud is the conventional cloud, which has amounts of computing ability, storage space and bandwidth. But it has a large latency. RSU-based cloud is the local cloud, which is close to the end user. It has limited resource of computation, storage and bandwidth, compared to the Internet-based cloud. But it has a lower latency. Vehicle-based cloud is a temporary cloud, which consists of vehicles. Vehicle-based cloud plays a dual role: service provider and service consumer. Thus this cloud has very limited resource and the lowest latency.

In this chapter, we adopt a hybrid local cloud computing model, named joint RSU and vehicle-based cloud, which combines the RSU-based cloud and vehicle-based cloud. This model can bring the fixed RSU resource to the mobile vehicular resource. It reduces the impact of unstable nature from vehicles and latency of the RSU cloud. The existing three layers cloud model can still provide services in the high level. Fig. 6.2 shows that the Internet-based cloud is the highest level cloud. RSU cloud is in the middle level. The lowest level is the joint RSU and vehicle-based cloud.

Based on the joint RSU and vehicle-based cloud, we propose a new service named Spectrum Sensing as a Service (SSaaS), which can virtualize the vehicle in CR-VANETs to perform cooperative spectrum sensing. There are three distinguished advantages for vehicular virtualization in CR-VANETs as follows.

- Vehicles that need to perform cooperative spectrum sensing can obtain more computation and storage resources.
- Vehicles can join the spectrum sensing without contacting with other physical vehicles.
- SSaaS can automatically and ubiquitously find other vehicles when the specific vehicle is not available.

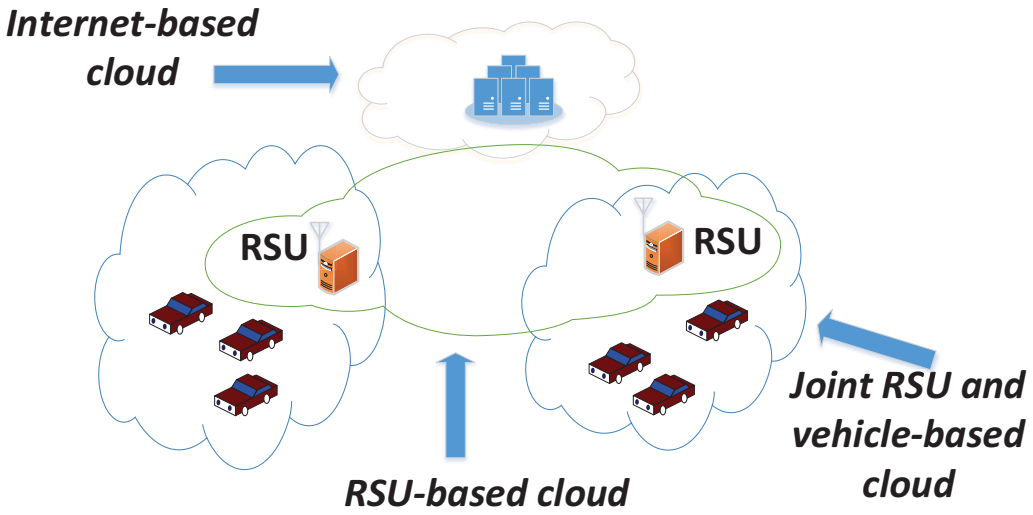

Figure 6.2: Joint RSU and vehicle-based cloud in CR-VANETs.

6.2.3 Security Issues in CR-VANETs

Security issues have been studied in spectrum sensing for several years. The incumbent emulation (IE) attack is proposed in [139]. In this attack, a malicious CR-enabled node mimics the PU's signal characteristics in order to interrupt the spectrum sensing process. The SSDF attack [121] is the most famous one, in which malicious SUs deliberately disseminate wrong sensing data to others so that the cooperative spectrum sensing is destroyed. For CR-VANETs, the SSDF is harder to be mitigated due to the mobility of each vehicle and limited resource for the protection of crypto-systems, such as public key infrastructure (PKI) based mechanisms.

In addition to the malicious attacks in the spectrum sensing phase, traditional security threats are still concerns in CR-VANETs, such as packet dropping attacks, also known as black hole attacks [19]. In this attack, the vehicle in the middle of the source and destination nodes can drop any packets, which need to be forwarded, including control packets and data packets.

6.3 Securing CR-VANETs with Trusted Lightweight Cloud Computing

Conventional consensus-based spectrum sensing requires physical nodes, such as vehicles, to work together. In CR-VANETs, during the spectrum sensing process, each vehicle has to stay in the local network. Another drawback is the limited resource of each physical vehicle. Each vehicle has different capability, e.g., computation, storage and bandwidth, to perform the spectrum sensing algorithm. To solve these issues, we present a cloud-based secure spectrum sensing for CR-VANETs, named SSaaS. This service is supported by the jointed RSU and vehicle-based cloud, which is described in Subsection 6.2.2. Firstly, we introduce the architecture of the SSaaS. Then we explain the general service deployment template for the SSaaS. Finally, the consensus-based spectrum sensing with trust is illustrated as a service deployment in the SSaaS.

6.3.1 Architecture of SSaaS

In order to leverage spectrum sensing in cloud computing, an architecture of SSaaS is presented in Fig. 6.3. the Northbound could be a user or application, which is interested in a service deployment in the SSaaS. The Southbound could be any basic cloud computing platform such as OpenStack [36]. The SSaaS module provides core functions for spectrum sensing in CR-VANETs. The API between these three modules can be REST-enabled, which is popular in the cloud computing development community, or traditional library, which is embedded in the upper application software. In the SSaaS module, the VM controller orchestrates all the VMs in the service based on the service description in the template. For example, the VM locates in the specific host or which spectrum sensing algorithm is activated. The trust engine module provides a variety of trust mechanisms, which are used to assess the

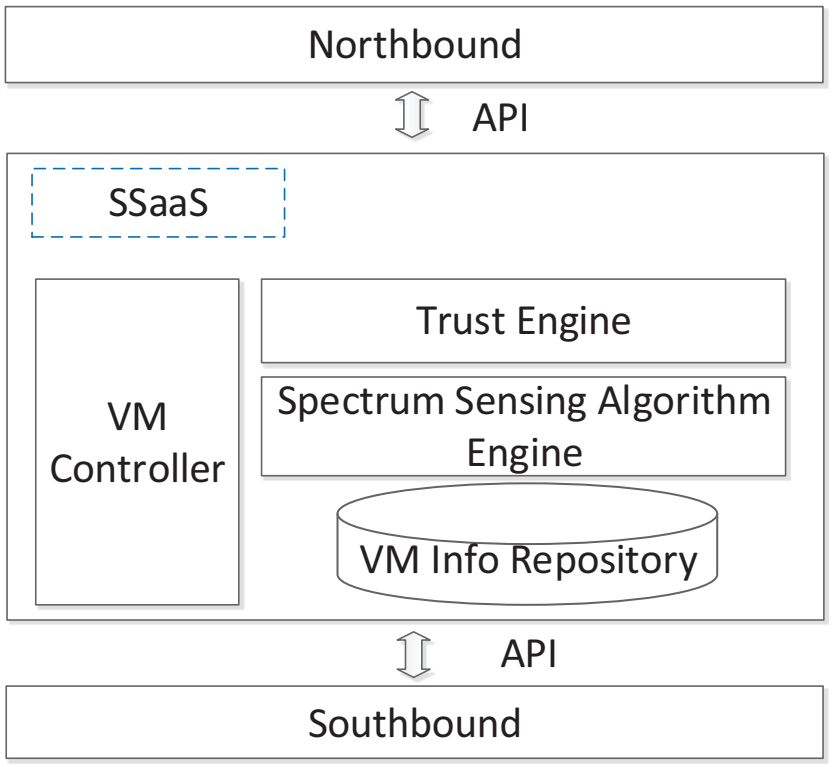

Figure 6.3: The architecture of SSaaS.

trustworthiness [106] of each vehicle. The spectrum sensing algorithm engine is in charge of the specific spectrum sensing, which is selected in the service deployment. The VM info repository stores the specific service deployment details.

6.3.2 SSaaS Service Deployment Template

A user or application that needs to use SSaaS can define a detailed service deployment with a template, which is similar to the conventional cloud service deployments [140]. We format the template with JSON [141], which is not only processed by most modern programming languages but also friendly for human-reading. Fig. 6.4 shows an SSaaS deployment from Northbound. In this service deployment, the number of servers is defined that how many VMs join together to perform cooperative spectrum sensing. Context is used to describe the network environment. The spectrum sensing algorithm specifies the scheme for spectrum sensing in the service. The trust algorithm defines the trust scheme that trust engine will processes. We will explain it with more details in the next subsection.

6.3.3 Consensus-based Spectrum Sensing with Trust

There are two important parts in this scheme. Firstly, the consensus-based spectrum sensing is introduced. Secondly, trust scheme can assist the consensus-based spectrum sensing, where trust is considered as the weight.

Here we formulate a CR-VANET as an undirect simple graph, G. This graph is represented by a matrix $A = (a_{ij})_{n\times n}$, where

$$a_{ij} = \begin{cases} 1, & \text{if } j \in N(i) \\ 0, & \text{otherwise} \end{cases} \tag{6.1}$$

```
{"SSaaS":{
    "name":"CR-VANETs-dep",
    "user":"user-a",
    "server_list":{
      "name":"list-1",
      "image":"ubuntu",
      "flavor":"mini",
      "number_of_server":{
      "min":6,
      "max":10
      },
      "context":"cr-vanet",
      "spectrum_sensing_algorithm":{
        "name":"consensus-based with trust",
        "trust_algorithm":"Bayesian",
      }
    }
    ...
  }
}
```

Figure 6.4: SSaaS service deployment template in JSON.

where $N(i)$ is a one-hop neighbor set of vertex i.

The weighted-average consensus [127, 128] is listed as follows:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in N_i(k)} w_{ij}(x_j(k) - x_i(k)), \tag{6.2}$$

where $0 < \epsilon < (\max_i |N_i|)^{-1}$, w_{ij} is a weight for CR vehicle i to its neighbor. Here the weight is the function of trust value of each neighbor. It is defined as

$$w_{ij} = \frac{T_{ij}}{1 + \sum_{j \in N(i)} T_{ij}}. \tag{6.3}$$

When $k \to \infty$ in (6.2), $x_i(k) \to x^*$ [128].

The basic procedure based on (6.2) is described as follows. At first, each virtual vehicle in the cloud service deployment, which is willing to perform cooperative spectrum sensing needs to use energy detection mechanism to explore the status of the PU. Once the status is obtained, virtual vehicles should exchange the status of the PU to each other. A virtual vehicle utilizes the sensing data received to update its value by (6.2). When calculation finished, the virtual vehicle will disseminate its current value to its one-hop neighbors. When the difference between the new result of each virtual vehicle and a common consensus value is less than or equal to a tolerant deviation, the iterating procedure is done. Virtual vehicles compare the value with a pre-defined threshold [61] to determine if the PU is present.

Trust is updated for each iterating step in the process. It reflects the real trust of neighbor virtual vehicles. However, it may cause the resource limitation issues and large latency for trust retrieving. In this chapter, we use the trust definition from [4], which is the degree of belief that an entity (virtual vehicle) can perform a duty as expected. It is denoted as $T \in [0, 1]$. Trust evaluation is employed, which is described in [142].

6.4 Simulation Results and Discussions

In this section, we present simulation results to show the effectiveness of the SSaaS in CR-VANETs when a malicious virtual vehicle continuously reports wrong sensing data in order to interfere the cooperative sensing. Then the probability of success is illustrated. Finally, the latency in the cloud computing is showed in the experiments.

6.4.1 SSaaS Versus SSDF

There are six virtual vehicles in the service deployment. There is one PU in the network. Through the cooperative spectrum sensing, the SSaaS finally provides the status of the PU. Then the user or application can decide to use the licensed spectrum band based on the result from the SSaaS. In the simulation, we assume that the malicious virtual vehicle is always existing. The pre-defined threshold of PU presence is $\lambda = 11.4dB$. During the consensus-based cooperative spectrum sensing, the malicious virtual vehicle sends dynamic wrong sensing data to interrupt the spectrum sensing procedure. Fig. 6.5 shows that trust scheme can exclude the impact from the malicious virtual vehicle. The consensus result can be achieved among the normal virtual vehicles. Then the correct decision that the PU is present is made by the SSaaS. In Fig. 6.6, virtual vehicle 3 becomes an attacker. When two malicious virtual vehicles perform attacks with variable incorrect sensing data, the proposed service still works but the converging progress becomes slow in the simulations. In addition, simulation results show that the SSaaS is effective when the number of malicious virtual vehicles is minor in the entire virtual vehicle server list.

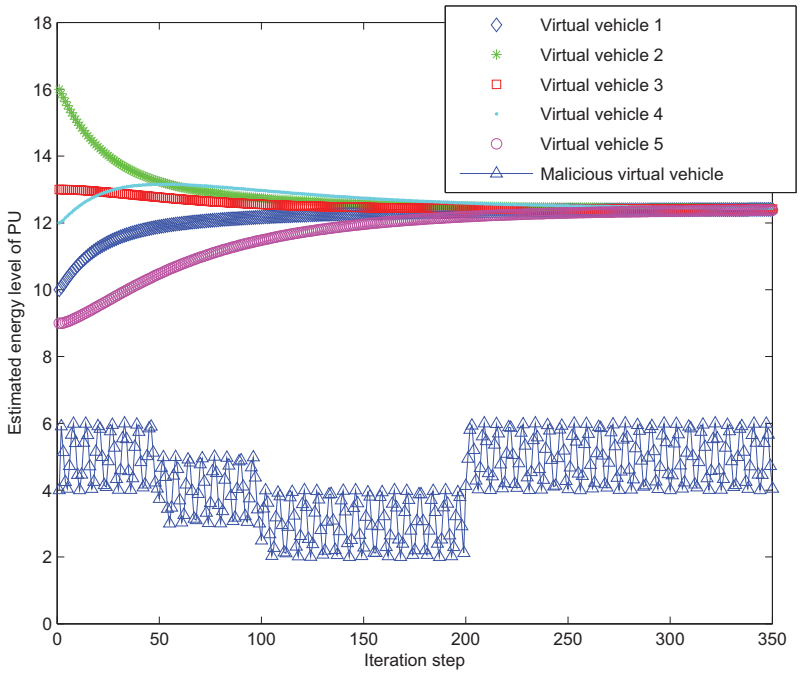

Figure 6.5: SSaaS with one malicious virtual vehicle.

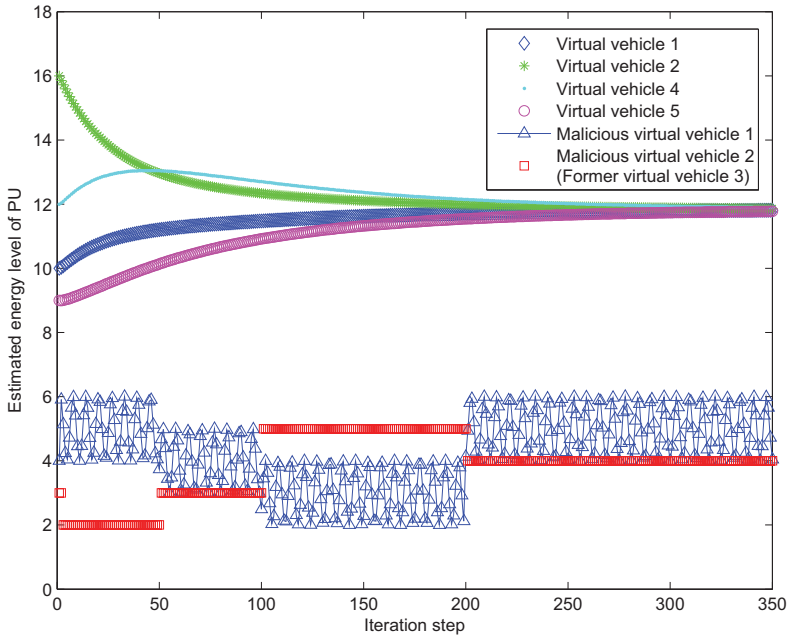

Figure 6.6: SSaaS with two malicious virtual vehicle.

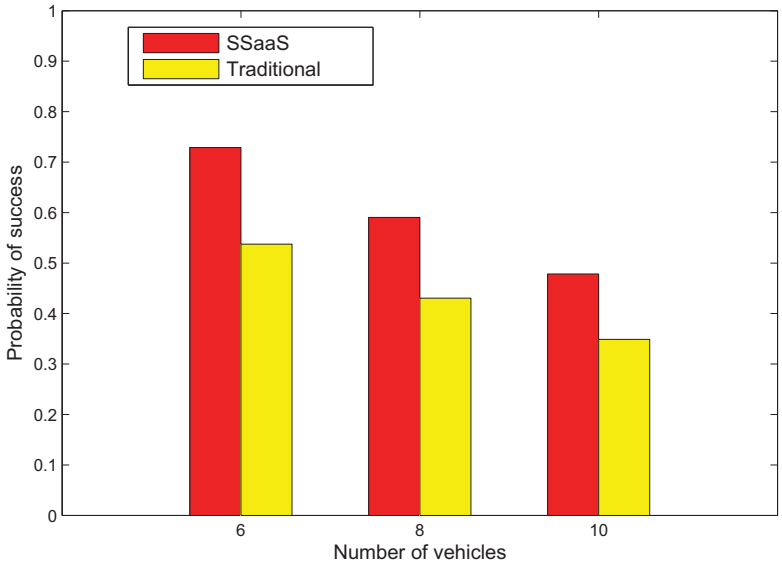

Figure 6.7: Performance comparison in terms of the probability of success.

6.4.2 Probabilities of Success

The benefit of the SSaaS is that the physical vehicle is virtualized in the service deployment. That means the user or application has no awareness of the real vehicles that perform spectrum sensing. The virtual vehicle can reside in the different hosts. This can utilize the resource in different hosts that have more resources, such as power, computation capability, storage etc. We compare the traditional cooperative spectrum sensing and SSaaS in terms of the probability of success, which is defined as the probability that vehicles can perform cooperative spectrum sensing successfully and reach a finally decision, denoted as P_s. The availability of physical vehicles is P_{av}. Here, we assume $P_{av} \in [0.6, 0.9]$. Fig. 6.7 shows that SSaaS has higher probabilities than traditional physical vehicles. This is because that virtual vehicles can be deployed to the host that has the high availability. During the spectrum sensing procedure, the VM also can be seamlessly migrated to different hosts without interrupting the ongoing procedure thanks to the proposed lightweight cloud.

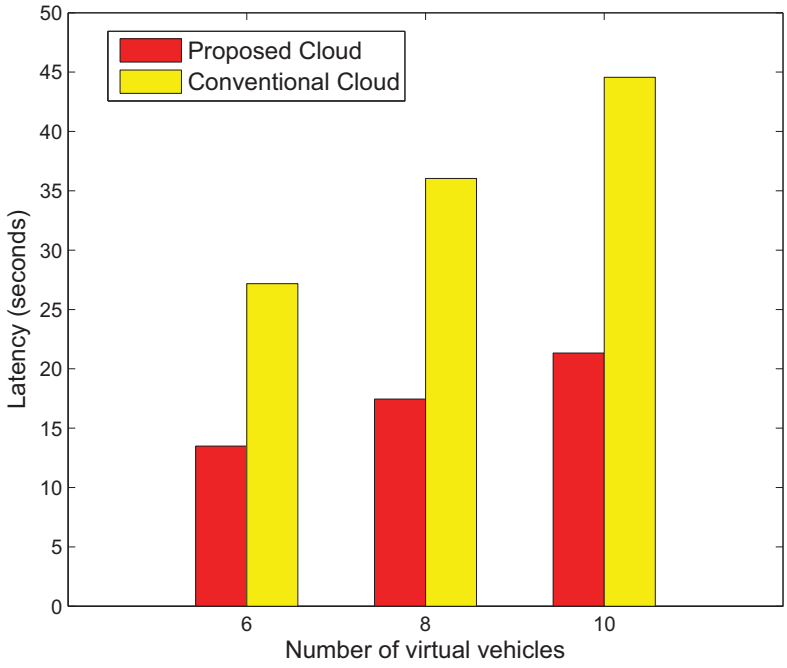

Figure 6.8: Latency in the proposed and conventional cloud.

6.4.3 Latency Improvement

Due to the dynamic nature of CR-VANETs, the localized cloud computing is more suitable than conventional Internet-based cloud. Here we evaluate the proposed lightweight cloud and Internet-based cloud with SSaaS service deployment in terms of number of VMs. In Fig. 6.8, as the number of VMs increases, the latency becomes larger gradually. This is because each VM needs to fetch the trust from the cloud. Then the more VMs joints the cooperative spectrum sensing, the larger latency is generated. The communication time between VMs is also increased as the number of VMs increases. The latency in the conventional cloud is larger than the proposed one, almost two times. The retrieving process in the Internet-based data centers needs more time in the experiments.

6.5 Chapter Summary

CR-VANETs have become a promising technology for driving safety and entertainment in connected vehicles. Security is the key to the success of connected vehicles. To solve the security issues of cooperative spectrum sensing in CR-VANETs, spectrum sensing as a service was proposed in this work, which is based on the joint RSU and vehicle-based local cloud computing model. Through the deploying service in the cloud, a safe consensus-based cooperative spectrum sensing is applied. The effectiveness of this cloud-based spectrum sensing scheme is verified by the simulation results. It was shown that the cloud computing in CR-VANETs can effectively reduce latency and improve the security of CR-VANETs.

Chapter 7

Conclusions and Future Work

In this dissertation, we have thoroughly studied the security issues, the inside attacks, on four ad hoc networking paradigms including MANETs, tactical MANETs, CR enabled ad hoc networks, and VANETs with NFV. The security issues are mitigated and tackled by the advances of uncertain reasoning in trust management. In this chapter, we conclude the accomplished works and present some possible research directions in the future.

7.1 Summary

The proposed schemes in Chapter 3, 4, 5, and 6 address the inside attacks with trust management by the Bayesian inference, DST, and the Bayesian networks model. In a nutshell, we have studied and accomplished the following:

- In Chapter 3, we proposed a unified trust management scheme that enhances the security of MANETs. Using recent advances in uncertain reasoning, Bayesian inference and Dempster-Shafer theory, we evaluated the trust values of observed nodes in MANETs. Misbehavior such as dropping or modifying packets can be detected in our scheme through trust values by direct and indirect observation. Nodes with low trust values will be excluded by the routing algorithm.

Therefore, secure routing path can be established in malicious environments. Based on the proposed scheme, more accurate trust can be obtained by considering different types of packets, indirect observation from one-hop neighbors and other important factors such as buffers of queues and states of wireless connections, which may cause dropping packets in friendly nodes. The results of MANET routing scenario positively support the effectiveness and performance of our scheme, which improves throughput and packet delivery ratio considerably, with slightly increased average end-to-end delays and overhead of messages.

- In Chapter 4, we proposed a trust-based scheme that utilizes Bayesian networks, which has advantages in causal reasoning with probability and graph theories. Depending on causal relationships in the Bayesian network, our scheme can obtain a more accurate trust value by differentiating malicious behavior. As a result, the throughput performance of MANETs with the consideration of a variety of causes for packets dropping can be improved, and the false alarm probability of the proposed scheme is low.

- In Chapter 5, we introduced a new attack, named joint spectrum sensing and data transmission (JSSDT) attack, which can dramatically disrupt the normal functions of CR-MANETs. Using recent advances in the theory of uncertain reasoning, we developed a unified trust management scheme with both direct observation and indirect observation. Based on the unified trust model, we presented a scheme to protect both spectrum sensing and data transmission processes. Simulation results demonstrated the effectiveness of the proposed schemes in CR-MANETs.

- In Chapter 6, to solve the security issues of cooperative spectrum sensing in CR-VANETs with NFV, spectrum sensing as a service was proposed in this chapter, which is based on the joint RSU and vehicle-based local cloud computing model. Through the deploying service in the cloud, a safe consensus-based cooperative spectrum sensing is applied. The effectiveness of this cloud-based spectrum sensing scheme is verified by the simulation results. It was shown that the cloud computing in CR-VANETs can effectively reduce latency and improve the security of CR-VANETs.

7.2 Future Work

Based on the accomplished research works, there are several important research problems in the emerging ad hoc networking paradigms. We outline them as follows.

- Trust is the core of this research. Trust evaluation is formulated by Bayesian probability, which is based on the evidence. In order to obtain more accurate trust, a new calculation algorithm based on large evidence is needed. Based on the advance of big data analytics and cloud computing technology, the Bayesian methodology for trust can be improved and developed. This interesting and meaningful research direction can be explored.

- For the schemes presented, we assume that self-organized nodes can be seized by a malicious attacker. However, each node is independent. In other words, there is no collusion between two or more nodes. This is a simple scenario for the inside attacks. To some extent, trust for this sole criminal is obtained and calculated relatively much easier than that for a gang of villains. In order to tackle this complicated attack pattern, a new trust management for a group of malicious nodes needs to be investigated.

- NFV is the promising technology that can abstract the networking functions and make the installation and configuration easily and flexibly so that the administrators can extend the network service following the dynamical requirements from end users. This merit is being achieved by both academia and industry efforts. The security issues of virtualization [143] and cloud computing [144] in CR-VANETs, such as how to find the safe host during vehicular virtual machine migration [45] and high availability [29], should be studied further.

List of References

[1] "Network functions virtualisaztion (NFV); NFV security; problem statement." website: http://www.etsi.org.

[2] "Network functions virtualisaztion (NFV): Architectural framework." website: http://www.etsi.org.

[3] M. Weiser, "The computer for the 21st century," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 3, pp. 3–11, July 1999.

[4] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[5] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," *IETF RFC 3626*, Oct. 2003.

[6] T. Clausen, C. Dearlove, and P. Jacquet, "The optimized link state routing protocol version 2," *IETF draft-ietf-manet-olsrv2-13*, Oct. 2011.

[7] "Qualnet simulator." website: http://www.scalable-networks.com/content/.

[8] D. Heckerman, "A tutorial on learning with bayesian networks," *Microsoft Research Report MSR-TR-95-06*, 1995.

[9] M. Momani, S. Challa, and R. Alhmouz, "BNWSN: Bayesian network trust model for wireless sensor networks," in *Proc. MIC CCA'08*, (Amman), Aug. 2008.

[10] C. T. Nguyen, O. Camp, and S. Loiseau, "A Bayesian network based trust model for improving collaboration in mobile ad hoc networks," in *Proc. IEEE Research, Innovation and Vision for the Future*, (Hanoi, Vietnam), Mar. 2007.

[11] Y. Wang and J. Vassileva, "Bayesian network trust model in peer-to-peer networks," in *Proc. AAMAS'03*, (Melbourne, Australia), Jul. 2003.

[12] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann, 1988.

[13] G. Shafer and J. Pearl, *Readings in Uncertain Reasoning*. Morgan Kaufmann, 1990.

[14] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proc. ACM AAMAS'02*, (Bologna, Italy), Jul. 2002.

[15] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using Dempster-Shafer theory," in *Proc. IEEE Instrumentation and Measurement Technology Conf.*, (Alaska, USA), May 2002.

[16] J. Y. Halpern, *Reasoning about Uncertainty*. The MIT Press, 2003.

[17] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Proc. IEEE MilCom'09*, (Boston, MA, USA), Oct. 2009.

[18] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *Mobile Ad Hoc Networking: The Cutting Edge Directions, 2nd Edition*. Wiley-IEEE Press, 2013.

[19] J. Loo, J. Lloret, and J. H. Ortiz, *Mobile Ad Hoc Networks: Current Status and Future Trends*. CRC Press, 2011.

[20] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for ipv4," *IETF RFC 4728*, Feb. 2007.

[21] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," *IETF RFC 3561*, Jul. 2003.

[22] T. Clausen, C. Dearlove, and J. Dean, "Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)," *IETF RFC 6130*, Apr. 2011.

[23] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR protocol," in *Proc. 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2003)*, (Mahdia, Tunisia), Jun. 2003.

[24] T. Clausen and U. Herberg, "Vulnerability analysis of the optimized link state routing protocol version 2 (OLSRv2)," in *Proc. IEEE WCNIS'10*, (Beijing, China), Feb. 2010.

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

[26] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: distributed key management for security," in *Proc. 2nd OLSR Workshop*, (Domaine de Voluceau, France), Dec. 2005.

[27] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, and A. A. Loureiro, "Data communication in vanets," *Ad Hoc Netw.*, vol. 44, pp. 90–103, July 2016.

[28] J. M. III, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*. KTH, 2000.

[29] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, pp. 50–58, Apr. 2010.

[30] "Dropbox." https://www.dropbox.com.

[31] "Github." https://github.com/.

[32] "Google app engine." https://cloud.google.com/appengine/docs.

[33] "Microsoft azure." https://azure.microsoft.com/en-us/?b=16.44.

[34] R. P. Goldberg, "Survey of virtual machine research," *Computer*, vol. 7, pp. 34–45, Sep. 1974.

[35] M. Gozani, *Network Virtualization for Dummies (VMware Special Edition)*. John Wiley & Sons, Inc., 2016.

[36] "Openstack cloud computing software." website: https://www.openstack.org/.

[37] "VMware vCentre." website: http://www.vmware.com/ca/products/vcenter-server.html.

[38] "AWS." website: https://aws.amazon.com/.

[39] S. Bitam, A. Mellouk, and S. Zeadally, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Wireless Communications*, vol. 22, pp. 96–102, Feb. 201.

[40] E. Lee, E. K. Lee, M. Gerla, and S. Y. Oh, "Vehicular cloud networking: architecture and design principles," *IEEE Commun. Magazine*, vol. 52, pp. 148–155, Feb. 2014.

[41] Q. Yang, B. Zhu, and S. Wu, "An architecture of cloud-assisted information dissemination in vehicular networks," *IEEE Access*, vol. 4, pp. 2764–2770, May 2016.

[42] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *arXiv:1308.6208v1*, Aug. 2013.

[43] N. Cordeschi, D. Amendola, and E. Baccarelli, "Reliable adaptive resource management for cognitive cloud vehicular networks," *IEEE Trans. Veh. Tech.*, vol. 64, pp. 2528 –2537, Jun. 2015.

[44] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. of the 2014 Federated Conference on Computer Science and Information Systems*, (Warsaw, Poland), Sept. 2014.

[45] B. Baron, M. Campista, P. Spathis, L. Costa, M. Amorim, O. Duarte, G. Pujolle, and Y. Viniotis, "Virtualizing vehicular node resources: feasibility study of virtual machine migration," *to be submitted to Vehicular Communications Journal*, May 2016.

[46] S. Bu, F. Yu, P. Liu, P. Mason, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high security mobile ad-hoc networks," *IEEE Trans. Veh. Tech.*, vol. 60, no. 3, pp. 1025–1036, 2011.

[47] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proceedings of the IEEE*, vol. 100, pp. 3172–3186, Dec 2012.

[48] R. Chen, J.-M. Park, and B. Kaigui, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM'08*, (Phoenix, AZ, USA), Apr. 2008.

[49] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowdsourcing spectrum data in white space networks," in *Proc. IEEE DySPAN'2010*, (Singapore), Apr. 2010.

[50] H. Li and Z. Han, "Catch me if you can: an abnomility detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, 2010.

[51] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, 2010.

[52] W. Wang, H. Li, Y. Sun, and Z. Han, "Catch it: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE GLOBECOM'09*, (Honolulu, HAWAI, USA), Nov. 2009.

[53] A. Hafslund, A. Tonnesen, R. B. Rotvik, J. Andersson, and O. Kure, "Secure extension to the OLSR protocol," in *Proc. OLSR Interop and Workshop*, (San Diego, CA, USA), Aug. 2004.

[54] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no. 1, pp. 21–38, 2005.

[55] S. Marti, T. Giuli, K. Lai, and M. Maker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MobiCom'00*, (New York, NY, USA), Aug. 2000.

[56] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol," in *Proc. ACM MOBIHOC'02*, (Lausanne, Switzerland), Jun. 2002.

[57] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. 3rd ACM Workshop on SASN'05*, (Alexandria, VA, USA), Nov. 2005.

[58] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, 2006.

[59] H. Deng, Y. Yang, G. Jin, R. Xu, and W. Shi, "Building a trust-aware dynamic routing solution for wireless sensor neworks," in *Proc. IEEE GLOBECOM'10 Workshop on Heterogeneours, Multi-hop Wireless and Mobile Networks*, (Miami, FL, USA), Dec. 2010.

[60] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad-hoc networks," *IET Inf. Secur.*, vol. 6, no. 2, pp. 77–83, 2012.

[61] Z. Li, F. R. Yu, and M. Huang, "A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios," *IEEE Trans. Veh. Tech.*, vol. 59, no. 1, pp. 383–393, 2010.

[62] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. T. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM'12*, (Orlando, FL, USA), Mar. 2012.

[63] L. R. Bays, R. R. Oliveira, M. P. Barcellos, L. P. G. author, and E. R. M. Madeira, "Virtual network security: threats, countermeasures, and challenges," *Journal of Internet Services and Applications*, vol. 6, no. 1, 2015.

[64] J. M. Gonzalez, M. Anwar, and J. B. Joshi, "Trust-based approaches to solve routing issues in ad-hoc wireless networks: A survey," in *Proc. IEEE TrustCom'11*, (Ciudad Real, Spain), Apr. 2011.

[65] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 14, pp. 279–298, May 2012.

[66] M. Deutch, "Cooperation and trust: Some theoretical notes," in *Nebraska Symposium on Motivation*, p. 275319, 1962.

[67] J. Golbeck, "Computing with trust: Definition, properties, and algorithms," in *2006 Securecomm and Workshops*, pp. 1–7, Aug 2006.

[68] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, (Washington, DC, USA), IEEE Computer Society, 1996.

[69] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems*, (Bologna, Italy), Nov. 2004.

[70] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 35–41, 2005.

[71] W. Li and A. Joshi, "Outlier detection in ad hoc networks using Dempster-Shafer theory," in *Proc. MDM'09*, (Taipei, Taiwan), May 2009.

[72] Z. Zhao, H. Hu, G.-J. Ahn, and R. Wu, "Risk-aware mitigation for manet routing attacks," *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 2, pp. 250–260, 2012.

[73] A. Boukercha, L. Xua, and K. EL-Khatibb, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, vol. 30, pp. 2413–2427, Sep. 2007.

[74] A. Boukercha and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," *Computer Communications*, vol. 31, pp. 4343–4351, Dec. 2008.

[75] A. Boukerche and X. Li, "An agent-based trust and reputation management scheme for wireless sensor networks," in *GLOBECOM '05. IEEE Global Telecommunications Conference, 2005.*, (St. Louis, MO, USA), Nov 2005.

[76] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," in *IEEE ICC '08*, (Beijin, CHINA), May 2008.

[77] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 387–399, May 2009.

[78] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM SASN'04*, (Washington, D.C., USA), Oct. 2004.

[79] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM'08*, (Phoenix, AZ, USA), Mar. 2008.

[80] R. Changiz, H. Halabian, F. R. Yu, I. Lambadaris, H. Tang, and P. Mason, "Trust establishment in cooperative wireless networks," in *Proc. IEEE Milcom'10*, (San Jose, CA, USA), Nov. 2010.

[81] S. Jana, K. Zeng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," in *Proc. IEEE INFOCOM'12*, (Orlando, FL, USA), Mar. 2012.

[82] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile

ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 3064 –3073, Sept. 2011.

[83] L. Wasserman, *All of Statistics: A Concise Course in Statistical Inference*. Springer, 2004.

[84] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability, Second Edition*. Athena Scientific, 2008.

[85] Y. Beghriche, V. Toubiana, and H. Labiod, "A bayesian filter to detect misbehaving nodes in manets," in *Proc. NTMS'08*, (Tangier, Morocco), Nov. 2008.

[86] B. Elizabeth, R. Aaishwarya, P. Kiruthika, M. Shrada, A. Prakash, and V. Uthariaraj, "Bayesian based confidence model for trust inference in manets," in *Proc. IEEE ICRTIT'11*, (Chennai, Tamil Nadu, India), Jun. 2011.

[87] M. Mehdi, N. Bouguila, and J. Bentahar, "A QoS-based trust approach for service selection and composition via bayesian networks," in *Proc. IEEE ICWS'13*, (Santa Clara, CA, USA), Jun. 2013.

[88] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations," *IETF RFC 2501*, Jan. 1999.

[89] J. Chapin and V. W. Chan, "The next 10 years of DoD wireless networking research," in *Proc. IEEE Milcom'11*, (Baltimore, MD, USA), Nov. 2011.

[90] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable and Secure Computing*, vol. 3, pp. 386–399, Oct.–Dec. 2006.

[91] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Comm.*, vol. 16, no. 2, pp. 24–30, 2009.

[92] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: improving network security by multipath routing in mobile ad hoc networks," *ACM Wireless Networks*, vol. 15, no. 3, pp. 279–294, Mar. 2009.

[93] R. Zhang, Y. Zhang, and Y. Fang, "AOS: An anonymous overlay system for mobile ad hoc networks," *ACM Wireless Networks*, vol. 17, no. 4, pp. 843–859, May 2011.

[94] P. Albers, O. Camp, J.-M. Percher, B. Jouga, and L. M. R. S. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in *Proc. 1st Int'l Workshop on Wireless information Systems*, (Ciudad Real, Spain), Apr. 2002.

[95] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Comm.*, vol. 11, pp. 48–60, Feb. 2004.

[96] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey on trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[97] H. Kobayashi, B. L. Mark, and W. Turin, *Probability, Random Processes, and Statistical Analysis*. Cambridge University Press, 2011.

[98] Y. Owada, T. Maeno, and H. Imai, "OLSRv2 implementation and performance evaluation with link layer feedback," in *Proc. ACM IWCMC'07*, (Honolulu, Hawaii, USA), Aug. 2007.

[99] C. Dearlove, T. Clausen, and P. Jacquet, "Link metrics for olsrv2," *IETF draft-dearlove-olsrv2-metrics-05*, Jun. 2010.

[100] "Trust platform module." website: http://www.trustedcomputinggroup.org/.

[101] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. IEEE International Conference on Network Protocols (ICNP)*, (Paris, France), Nov. 2002.

[102] J. Liu, F. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 806–815, 2009.

[103] Q. Guan, F. Yu, S. Jiang, and V. Leung, "Joint topology control and security in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Tech.*, vol. 61, no. 6, pp. 2674–2685, 2012.

[104] Y. Wang, F. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627, 2014.

[105] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *Mobile Ad Hoc Networking*. Wiley-IEEE Press, 2004.

[106] Z. Wei, H. Tang, F. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Trans. Veh. Tech.*, vol. 63, no. 9, pp. 4647–4658, Feb. 2014.

[107] A. Darwiche, *Modeling and reasoning with Bayesian Networks*. Cambridge University Press, 2009.

[108] Y. Cho and G. Qu, "Enhancing trust-aware routing by false alarm detection and recovery," in *Proc. IEEE MILCOM'14*, (Baltimore, MD, USA), Oct. 2014.

[109] F. V. Jensen and T. D. Nielsen, *Bayesian Networks and Decision Graphs*. Springer, 2007.

[110] E. Charniak, "Bayesian networks without tears," *AI Magazine*, vol. 12, no. 4, pp. 50–63, 1991.

[111] N. Fenton and M. Neil, *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press, 2012.

[112] J. B. Schafer, J. Konstan, and J. Riedl, "Recommender systems in e-commerce," in *Proc. ACM EC '99*, (Denver, Colorado, USA), 1999.

[113] D. Koller and N. Friedman, *Probabilistic Graphical Models: Principles and Techniques*. The MIT Press, 2009.

[114] Z. Wei, H. Tang, F. R. Yu, and M. Wang, "Security enhancement for mobile ad hoc networks routing with OLSRv2," in *Proc. SPIE Defence, Security, and Sensing 2013*, (Baltimore, MD, USA), Apr. 2013.

[115] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[116] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, pp. 2127–2159, 2006.

[117] F. R. Yu, *Cognitive Radio Mobile Ad Hoc Networks*. New York: Springer, 2011.

[118] H. Yue, M. Pan, Y. Fang, and S. Glisic, "Spectrum and energy efficient relay station placement in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 883–893, May 2013.

[119] Y.-C. Liang, Y. Zeng, E. C. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, 2008.

[120] Q. Guan, F. R. Yu, S. Jiang, and G. Wei, "Prediction-based topology control and routing in cognitive radio mobile ad hoc networks," *IEEE Trans. Veh. Tech.*, vol. 59, pp. 4443 –4452, Nov. 2010.

[121] R. Chen, J.-M. Park, and Y. T. Hou, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Comm. Mag.*, April 2008.

[122] B. J. Chang and S. L. Kuo, "Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs," *IEEE Trans. Veh. Tech.*, vol. 58, pp. 1846–1863, Sept. 2009.

[123] R. Changiz, H. Halabian, F. R. Yu, I. Lambadaris, and H. Tang, "Trust establishment in cooperative wireless relaying networks," *Wireless Communications and Mobile Computing*, 2012.

[124] K. C. Chen, Y. J. Peng, N. Prasad, Y. C. Liang, and S. Sun, "Cognitive radio network architecture: part ii - trusted network layer structure," in *Proc. of the 2nd international conference on Ubiquitous information management and communication*, (New York, NY, USA), Apr. 2008.

[125] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE DySPAN'2005*, (Baltimore, MD, USA), Nov. 2005.

[126] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[127] Z. Tian, "Compressed wideband sensing in cooperative cognitive radio networks," in *Proc. IEEE GLOBECOM'08*, (New Orleans, LA, USA), Nov. 2008.

[128] L. Moreau, "Stability of multiagent systems with time-dependent communication links," *IEEE Trans. Auto. Control*, vol. 50, pp. 169–181, Feb. 2005.

[129] K.-C. Chen, P.-Y. Chen, N. Prasad, Y.-C. Liang, and S. Sun, "Trusted cognitive radio networking," *Wireless Communications and Mobile Computing*, vol. 10, no. 4, pp. 467–485, 2010.

[130] F. R. Yu, M. Huang, and H. Tang, "Biologically inspired consensus-based spectrum sensing in mobile ad hoc networks with cognitive radios," *IEEE Network*, vol. 24, pp. 26 –30, May 2010.

[131] F. R. Yu, "Connected vehicles for intelligent transportation systems," *IEEE Trans. Veh. Tech.*, vol. 65, pp. 3843–3844, June 2016.

[132] J. F. Bravo-Torres, M. Lpez-Nores, Y. Blanco-Fernndez, J. J. Pazos-Arias, M. Ramos-Cabrer, and A. Gil-Solla, "Optimizing reactive routing over virtual nodes in VANETs," *IEEE Trans. Veh. Tech.*, vol. 65, pp. 2274–2294, Apr. 2016.

[133] C. Luo, F. R. Yu, H. Ji, and V. Leung, "Distributed relay selection and power control in cognitive radio networks with cooperative transmission," in *Proc. IEEE ICC'10*, May 2010.

[134] F. Wang, H. Tang, F. R. Yu, and P. C. Mason, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," in *Proc. IEEE Milcom'09*, (Boston, MA, USA), Oct. 2009.

[135] S. Moursi and M. ElNainay, "A multi-metric routing protocol with service differentiation for cognitive radio ad-hoc networks," in *Proceedings of the 16th ACM International Conference on Modeling, Analysis, Simulation of Wireless and Mobile Systems*, MSWiM '13, (New York, NY, USA), pp. 129–134, ACM, 2013.

[136] J. Riihijärvi, J. Nasreddine, and P. Mähönen, "Influence of spatial statistics of spectrum use on the performance of cognitive wireless networks," in *Proc. 15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, MSWiM '12, (New York, NY, USA), pp. 5–14, ACM, 2012.

[137] G. Li, Z. Gu, X. Lin, H. Pu, and Q. Hua, "Deterministic distributed rendezvous algorithms for multi-radio cognitive radio networks," in *Proceedings of the 17th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, MSWiM '14, (New York, NY, USA), pp. 313–320, ACM, 2014.

[138] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Trans. Veh. Tech.*, vol. 65, pp. 3860–3873, June 2016.

[139] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, Jan. 2008.

[140] "Heat: OpenStack orchestration." website: https://wiki.openstack.org/wiki/Heat.

[141] "Javascript object notation." website: http://www.json.org/.

[142] Z. Wei, F. R. Yu, and A. Boukerche, "Trust based security enhancements for vehicular ad hoc networks," in *Proc. ACM DIVANet'14*, (Montreal, Canada), Oct. 2014.

[143] C. Liang and F. R. Yu, "Wireless network virtualization: A survey, some research issues and challenges," *IEEE Commun. Surveys Tutorials*, vol. 17, pp. 358–380, Firstquarter 2015.

[144] Z. Yin, F. Yu, S. Bu, and Z. Han, "Joint cloud and wireless networks operations in mobile cloud computing environments with telecom operator cloud," *IEEE Trans. Wireless Commun.*, vol. 14, pp. 4020–4033, July 2015.