ZOU, XIAOCHENG, M.S. Ant-Based Evidence Distribution with Periodic Broadcast in Attacked Wireless Network. (2011)
Directed by Jing Deng. 58 pp.

In order to establish trust among nodes in large wireless networks, the trust certificates need to be distributed and be readily accessible. However, even so, searching for trust certificates can be delayed and costly especially when wireless network is under CTS jamming attack, in which the attacker jams the reception of a control packet termed clear-to-send, CTS. We believe the individual solution can lead us to solve the combined problem. Therefore, in this work, we investigate the delay and cost of searching a distributed certificate and the adverse effects of fabricated control packet attacks on channel throughput and delivery ratio respectively, and propose two techniques that can improve the efficiency of searching for such certificates in the network and mitigate the CTS jamming attack's effect. Evidence Distribution based on Periodic Broadcast (EDPB) is the first solution we present to help node to quickly locate trust certificates in a large wireless sensor network. In this solution, nodes carrying certificates periodically announce their existence. Such announcements, together with a swarm-intelligence pheromone update procedure, will leave traces on the nodes to lead query packets toward the certificate nodes. We then investigate the salient features of this schema and evaluate its performance in both static and mobile networks. This schema can also be used for other essential information dissemination in mobile ad hoc networks. The second technique, address inspection schema (AIS) addresses vulnerabilities in distribution coordinating function (DCF) defined in IEEE 802.11 standard. The AIS scheme allows nodes to detect the CTS jamming attack and mitigates its adverse effect. We then perform ns-2 simulations to evaluate the benefit of AIS.

ANT-BASED EVIDENCE DISTRIBUTION WITH PERIODIC BROADCAST IN ATTACKED WIRELESS NETWORK

by

Xiaocheng Zou

A Thesis Submitted to
the Faculty of the Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Greensboro
2011

Approved by

Committee Chair

To my parents.

APPROVAL PAGE

This thesis has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair ______________________________
Jing Deng

Committee Members ______________________________
Shan Suthaharan

____
Nancy Green

____
Date of Acceptance by Committee

____
Date of Final Oral Examination

ACKNOWLEDGEMENTS

First, I would like to express my deepest gratitude to my advisor, Dr. Jing Deng, who constantly inspires, encourages, and guides me through the problems in my research. His wisdom and kindness have motivated me all the years. This work would not be successful without his inspiration, encouragement, and support.

Besides, I would like to thank Dr. Shan Suthaharan and Dr. Nancy Green, my another two thesis committee who take their time to offer me valuable suggestions during my thesis defense.

I also want to say thank you to all the group members: Adam Wright, Nihar Kurapati, and Rahul Reddy Maram for their constructive suggestions in the design of our second proposed schema.

A special thanks goes to Jinni Su and Jiayao Li, for all the moral support during my hard times and for wonderful time we have experienced together. They are parts of my success.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Wireless Communication Network

Wireless Communication Network technologies are dramatically making progress in recent years because of their significant advantages of productivity and convenience. The major goal of wireless communication network is now to allow a user to have access to the capabilities of global networks at any time without regard to location or mobility. There are four categories of wireless communication network: cellular wireless networks, wireless local area networks (WLAN), Ultra-wideband (UWB), and ad hoc and sensor networks. Cellular systems have experienced exponential growth over the last decade and cellular phones have already become essential part of people's daily life in most parts of the world. Now, cellular system evolves into the three generation (3G) and beyond technique which provides people easy and quick accessibility to online resources at any location or time. In addition, WLAN is replacing wired networks in many homes, businesses, and campuses. However, many technical challenges, for example, security, remain in designing robust wireless networks. Security mechanisms are essential to protect data integrity and confidentiality, access control, authentication, quality of service, user privacy, and continuity of service which are also critical to protect basic wireless network functionality.

1.2 Wireless Sensor Network

With the advances in micro-electro-mechanical systems (MEMS) technology which enables the development of sensor node, wireless sensor network has gained popularity in recent years. These sensor nodes are small in size and have limited computing speed and memory size. In addition, they are equipped with transceiver unit which allows them to communicate with each other peers within a certain distance and sensor units that can sense, measure, and gather information from the environment. A wireless sensor network (WSN) is composed of a large number of sensor nodes which are pre-deployed so that they can collaborate with each other to perform certain functionalities. There are two categories of WSN, structured and unstructured [51]. Unstructured WSN is the one that a collection of sensor nodes are in random deployment, that requires network protocol and algorithm can process self-organizing capabilities. For a structured WSN in which sensor nodes are deployed in a pre-planned manner, fewer sensor nodes are needed since the position of each node is carefully designed. Both of them have common characteristics, infra-structureless which does not require pre-deployed infrastructures such as base-stations and central control.

Due to significant research and development effort in past few years, a wide variety of applications are built on WSN which are able to monitor a wide range of ambient conditions such as object movement, temperature, humidity, lighting, and noise level etc.[3]. Example of these WSN applications include:

- Battle surveillance (e.g. friendly forces, equipment and ammunition tracking)
- Environmental monitoring (e.g. Forest fire and flood detection)

- Health diagnostics (e.g. Telemonitoring of human physiological data)
- Home monitoring (e.g. Home automation)
- Other applications (e.g. Vehicle tracking and detection)

1.3 Security Issues in Large Wireless Networks

While a wide range of WSN applications serving in civilian, industrial, and military areas, they are exposing security and privacy issues since every sensor node that locates at a accessible deployment area becomes potential attack point and easily suffers either physical or logic attacks. More specifically, these potential attacks can be categorized as follows [27], common attacks, denial of service (DoS) attack, node compromise, impersonation attack, and protocol-specific attacks.

Because of open access characteristic of wireless communication, there are some specific attacks aim at communication channels. An adversary can easily gain access to private or sensitive information by monitoring transmitted packets between nodes (*Eavesdropping*). Intruder can capture compromise sensor nodes to attack WSN by intercept messages and then modify the messages' content (*Message Modification*) or by sending a fault-data packet resembling a legitimate packet (*Message Injection*). A malicious node can launch DoS attack by using hardware failures, software bugs, or any conditions. A DoS attack on WSN may take several forms: *node collaboration*, in which a group of malicious nodes acts purposely to prevent information from reaching certain regions of network; *jamming attack*, in which attacker occupy communication channel to prohibit nodes in certain areas from sending or receiving packets; *exhaustion of power*, in which an attacker repeatedly communicate with victim node to exhaust their power. The classic example of Impersonation attack, in which node illegitimately claims multiple identities, is Sybil attack. Internal protocols such as routing and IEEE 801.11 standard used in WSN are facing threats by subverted nodes which adopt complex attacking strategies. Any of attacking strategies falls into one following categories [20]: *Spoofed Routing* information which is used to corrupt routing table information, *Selective Forwarding* in which malicious node selectively drops certain packets and forwards some packets without raising suspicions, *Wormhole Attack* in which information captured in one location is sent to another location to replay it through wormhole link, *Hello Flood Attack* in which fake HELLO packet broadcasted during the deployment of network, *Acknowledgement Spoofing* creates false acknowledgement message.

Information Privacy

With more and more critical information delivered on these wireless networks, an adversary can easily gain access to sensitive information communicated between two nodes due to the nature of wireless communication. Usually, wireless networks would employ asymmetric key scheme to guard the information privacy. In asymmetric key scheme, there are two kinds of keys in network, private key and public key. The public keys are ready to accessible for all nodes in network, and the private key is kept secretly by the node itself. In oder to protect the confidentiality and integrity of message, node (sender) should encrypt message using public keys of receiver that will then decrypt message using its own private key. Normally, to avoid been intercepted by adversary, the public keys are released by trusted third party, certificate authority (CA) which will issue certificates for nodes to perform public key authentication.

Each certificate, signed by the CA, contains a public key and the identifier of a node. Each of the nodes only needs to carry the public key of the CA and authenticate the certificate of the public key. However, due to constraint of memory size and CPU speed, the unique CA in WSN could be a bottleneck, therefore, multiple certificate copies are placed randomly in the network. When a node needs to verify a public key, it will query its neighborhood for a certificate copy. This process may occur frequently in the network as moving/joining nodes try to authenticate each other. Therefore, the query complexity and cost for a certificate copy should be as low as possible.

Many techniques allow nodes to search for certificate copies. For example, a Time-To-Live (TTL) based flooding can be used, but this has been found to cause the broadcast storm problem [29]. In [17], a swarm-intelligence based scheme termed Ant-Based Evidence Distribution (ABED) was proposed. In ABED, query packets are treated as ants looking for food source. Reply packets with certificate copy are considered as ants returning with food. These packets (ants) leave traces for other querying packets (ants) to find the certificate copy (food source). As we will demonstrate in this work, such an approach does not work well in mobile and dynamic networks because traces can become invalid quickly.

Vulnerabilities In IEEE 802.11 Standard

As WSN applications performed desired operations and functions for its intended use, defending against Denial-of-Service (DoS) attack, which aims to disrupt network functionalities rather than steal sensitive information, become significant. One of prominent DoS attacks is deviating from IEEE 802.11 standard protocol [1] which employs distribution coordinating function (DCF) technique to coordinates medium access for contending nodes. DCF is in fact the carrier sense multiple access with collision avoidance (CSMA/CA) schema which employs RTS/CTS mechanism to combat the hidden/exposed terminal problems. In this scheme, communication goes through a sequence of control/data packet dialogues: Request-To-Send (RTS) packet, Clear-To-Send (CTS) packet, Data (DATA) packet, and Acknowledgement (ACK) packet. DCF allows different nodes in the network to have fair shares of the medium usage.

In order to avoid collisions by packet transmissions from different nodes at various locations, a special field termed Network Allocation Vector (NAV) is included in RTS, CTS, and ACK packets. After receiving the NAV values on these control packets, nodes can only use the channel after the NAV timer expired. While this technique works well in allowing nodes to reserve the channel, it also opens the door to malicious attackers or selfish nodes in the network to gain unfair access or prohibit other nodes from accessing the channel.

Researchers have identified several weaknesses that might be exploited by an attacker or a selfish user in the network. For example, a selfish node may choose a small interval time in the back-off procedure [32] or delaying SIFS (Short Inter Frame Spacing) interval time instead of DIFS (Distributed Inter Frame Spacing) between the process of exchanging frames [36]. This would always give the attacker itself a better chance of successful channel reservation. Similarly, it may also achieve the same goal by sending out fabricated control packets to interfere with other nodes . This is sometimes termed *intelligent jamming* [23,31], as compared to physical jamming [49].

Compared to jamming detection [42, 50] at the physical layer, detection of intelligent jamming is more challenging. Such jammings consume less energy for the attacker while achieving a similar result - denying all other nodes' access to the channel. Due to the lack of proper data-link layer authentication techniques, any node in network could send out control packets such as RTS, CTS, and ACK. With these packets, it could dominate the channel by assigning an arbitrarily large value of NAV. Fabricated RTS attacks can be detected as nodes can sense the status of the channel for the data packet transmission with a longer carrier sensing range, or lower sensing threshold [53]. Fabricated CTS or ACK attacks are more subtle. Among others, one difficulty of detecting such attacks is that these control packets do not carry the packet sender's ID [1].

Problem Setting

We consider the setting where a large number of sensors are deployed in an IEEE 802.11 wireless network and a number of certificate copies are randomly distributed in network to avoid failure work of CA caused by malicious attack. All the sensors collaborate together to perform certain tasks, which require highly safety and robust. To guarantee information transmitted over network is safety, node can not communicate with other node until they obtain the certificate of other node which significantly increases network overhead. Besides, there are a few undetected sensor nodes randomly distributed in network which violate with IEEE 802.11 standard and send out spoof control packets periodically that subsequently block certain region's traffic.

Goals and Restrictions

In recapitulation, let us state our goals for this thesis in a concise form:

- Design a technique that allow any node can efficiently locate the certificate.
- Propose a solution to detect jamming attacks and recover network throughput

On the flipside we have established some restrictions to make this thesis feasible:

- We only consider there is one malicious node in network.
- Our solution is designed only to detect CTS jamming attack.

1.4 Document Organization

The following paper is divided into four chapters followed by the references.

- Chapter II introduces the related work.
- Chapter III explains our schema and solution in detail.
- Chapter IV shows the simulations results to evaluate our work.
- Chapter V summarizes our work and discuss future works.

CHAPTER II

RELATED WORK

Our work is mostly related to swarm intelligence applied on routing design, distributed evidence management and protection from jamming attack on MAC layer. In this chapter, we discuss several related work in the following.

2.1 Routing Protocol Design with Swarm Intelligence

Swarm intelligence (SI) [21] is the property of a decentralized, self-organized system in which individual behavior arising from agent's interaction with its environment causes a group of agents to act as cohesively and highly self-organized. SI is often observed in nature, including ant colonies and bee swarming etc. In 1985, Craig Reynolds [38] proposed a flocking model that models coordinated animal motion such as bird flocks and fish schools. The generic simulated flocking creature is called boid and there are three simple steering behaviors that describe how an individual boid maneuvers based on the positions and velocities of its neighboring boids, namely *separation*, *alignment*, and *cohesion*. The *separation* behavior steers a boid to avoid crowding its local flockmates. The *alignment* behavior steers a boid towards the average heading of its local flockmates. The *cohesion* behavior steers a boid to move toward the average position of its local flockmates. These three steering behaviors, using information sensed only from other nearby boids, allowed flockmates to behavior cohesively.

Inspired by SI, a lot of research are devoted to design adaptive, decentralized, flexible and robust artificial systems in the past years. Research on ant-colony based swarm intelligence has been developed and often used in dynamic optimization problems, such as energy saving and routing optimization in WSN. The power of such an approach for routing optimization can be explained below: consider how a certain ant species find the shortest path to food source merely by laying and following pheromone on trials. In a simple case, ants starting from nest to search for food would leave pheromone on trials. While some trials go nowhere, others lead them to food sources especially when the ants come back with food. Other ants follow (or are attracted by) these pheromones on the trails. Based on this observation, three categories routing protocols in WSN, unicast, multicast, and anycast are investigated.

Ant-Colony-Based Routing Algorithm (ARA) [13] is the classical example of ant-based swarm intelligence unicast routing protocol. This protocol consists of three main phases, namely route discovery, route maintenance, and route failure handling. During routing discovery phase, forward ant (FANT) is boradcasted by the sender and will be relayed by intermediated nodes to exploring potential new route to destination and establishing the pheromone track to the sender and subsequently, backward ant (BANT) is released by destination to establish pheromone trace to the destination. Routes are maintained by subsequent data packets which are transmitted over network. Pheromone values are updated by reinforce rule in order to strength path. Meanwhile, pheromone behaviored like what it does in nature, its value is decreased by the time goes on. Routing failure, usually caused by node's mobility, is detected by lost acknowledgement. Building upon ant-colony based dynamic routing protocols, Garcia and Pedraza [12] proposed a rational swarm (SWARM) routing protocol which is able to pick up best route (less latency and good quality) among multiple routes and achieves good network load balancing. Jiang and Baras [17] adapt this ant-based algorithm to distribute trust evidence management in ad hoc networks. In their approach, query messages are considered as forward ants that may be broadcasted or unicasted. The return information are considered backward ants that leave traces for future forward ants to follow. However, communication cost and latency are high in their approach because many forward ants are likely to be broadcasted (flooded) in the neighborhood. Furthermore, complicated reinforcement rule can lead to trial loops in mobile networks, effectively eliminating the benefits of such traces.

To overcome overhead problem of unicast routing, Jeon and Kesidis [16] presented an ant-based multipath routing protocol that jointly manage both energy and latency concerns in a volatile networking context. Their approach operates similar manner to ARA, but with two exceptions. The first one is instead of discard duplicated FANTs, intermediate nodes relayed duplicated FANTs to build multiple routes from source to destination. Another one is pheromone level values are updated by energy and delay metrics rather than positive and negative feedback. Shen and Jaikaeo [41] proposed a novel multicast routing protocol for mobile ad hoc networks, Multicast for Ad Hoc Networks with Swarm Intelligence (MANSI), to establish multicast connectivity. In their schema, initial forwarding set, usually not optimized, will evolves into states that yield lower cost during the lifetime of the multicast session by deploying forward ant packet which is periodically sent out by non-core member and acts like an ant in real world to opportunistically explore different better paths to core.

Anycast routing protocol using swarm intelligence (ARPSI) is proposed by Hoh et al. [8] to route packets dynamically to a nearby server with low overhead in a mobile, ad hoc, wireless network by applying the behavior of the real ant colonies. Routing discovery and route maintenance are two phases of this system. During routing discovery phase, multiple paths from mobile node to anycast servers are established by exchanging QUERY and REPLY packets in which pheromone is laid on the path, so that anycast packets are efficiently routed to destination according to pheromone intensity. In route maintenance phase, EXPLORE packets are periodically sent to anycast server to monitor quality of existing routes and to explore new route.

To address power consumption issue in WSN, Shen et al. [40] proposed Ant-Based Topology Control (ABTC) algorithm to minimize the maximum power used by any node in network or minimize the total power used by all of the nodes in the network, while maintaining network connectivity. Their algorithm adapts the biological metaphor of swarm intelligence as a heuristic search mechanism and each node in network search a proper transmit power by collecting local information from its neighbors. In addition, Load Balancing and Energy ware ARAMA (LBE-ARAMA) routing [34] attempts to solve both energy saving and traffic load balancing issues by adopting different metrics and global and local parameters in their computation model.

Not only ant colonies behavior's principles are adopted in current research, other swarms' behavior such as honey bees are also investigated by researchers to solve real problems. BeeHive [47] is a routing protocol that achieves fault tolerant, scalability, and robust based on inspiration of communicative and evaluative methods and procedures of honey bees. Unlike Ant-based algorithm, this approach eliminates any global information such as topology structure and cost of links among routers, and global clock synchronization by working with local information which is collected by bee agent travels in a foraging zone. Based on swarm intelligence, specifically on honey bee colony, BeeAdHoc [46] is proposed as a novel routing protocol which mainly considers the power consumption concern. Two main types of packets, Scout and Forager are designed in this approach. Scout is used to discovery new routes on demand whereas Forger evaluates the quality of existing routes by transporting data packets from source to destination. This simplicity results in substantially smaller number of control packets sent, furthermore, the power consumption of network is optimized.

2.2 Evidence management in distributed environment

Efficient security mechanisms in distributed environment for trust management have been investigated through different perspectives since traditional security mechanisms for confidentiality and authentication cannot be employed directly. Abdul-Rahman and Hailes [2] proposed a distributed trust model with explicit trust statement to reduce ambiguity and recommended a protocol to exchange trust-related information. Zhou and Haas [54] introduced a key management scheme that distributively assigns trust and shares keys in a set of nodes to solve the vulnerability problem of a single CA in ad hoc networks. Capkun et al. [9] proposed a self-organizing public-key management system that allows users to fully control the security settings of the system without the help of any trusted authority or fixed server.

Ren et al. [37] proposed a reliable trust establishment scheme that uses secret dealer to construct trust relationship in the system bootstrapping phase. Then they adopted a fully self-organized trust establishment approach. A chained of peer nodes were used to bootstrap key distribution, with the help from mobile nodes, in [45]. A technique taking advantage of heterogeneous networks was proposed in [44]. An agent-based trust and reputation management scheme (ATRM) was introduced and evaluated in [7]. In [25], an on-demand public key management (OPKM) public key management scheme was proposed. The OPKM scheme makes use of broadcasting technology and digital signature for on-demand key management service.

Even when trust management is in place, it is still challenging for wireless nodes to retrieve and distribute trust evidence. This is because many wireless networks such mobile ad hoc networks (MANETs) are self-organized with vulnerable links. Flooding is a simple and straight-forward method to send out queries toward the certificate nodes. There have been many works trying to improve flooding efficiency. Cheng and Heinzelman [11] designed an optimal flooding strategy minimizing cost and latency for target discovery, although large amount of querying traffic and potential collisions will be generated, especially with multiple queries. Similar approaches were taken in peer-to-peer systems due to the similarities between such networks and ad hoc networks. For example, Passive Distributed Indexing(PDI) [26], based on peer-to-peer technology, addresses the file sharing problem in mobile scenarios by eliminating the need of flooding to the entire network.

Power consumption is yet another important issue. Many strategies for cache management have been proposed and studied with the objective of minimizing energy consumption and balancing network load. Barbara and Imielinski [5] proposed three strategies that use invalidation reports and a stateless server. Broadcasting Timestamps (BT) technique allows clients to report timestamp of each cached item to server which, in turn, updates timestamp or purges cached items according to report. In Amnesic Terminals (AT) strategy, the server actively informs nodes the identifiers of the items that changed since the last invalidation report. SIG is the third technique that focuses on a new protocol between server and clients by signing a set of cached items instead of just one item.

Jin and Wang [18] argued that demand-driven proportional strategy for replication is far from optimal in 2-D mesh. They proposed an optimal strategy that replicates an object such that the number of its replicas is proportional to $p^{0.667}$, where p is the access probability of the object in multi-hop wireless mesh networks. In [30], Nuggehalli et al. addressed the issue of energy-conscious cache placement in wireless ad hoc networks. While caching of information stored at the server on several distributed nodes can improve information access delay, the energy consumption can be much higher due to the delivery of such information to the caching locations. A polynomial time algorithm was designed to compute the sub-optimal caching locations [30]. In this paper, however, we are interested in the problem of lowering query overhead in mobile wireless networks.

The problem we are focusing on shares many similarities with data dissemination in wireless networks [15,52]. In fact, the certificate information we discuss in this work can be any other information that is needed throughout the network. Data caching can be used to improve the availability of essential information in the network [19, 22, 48, 52]. Besides, we take the jamming attack at MAC layer into consideration.

2.3 Jamming Detection at MAC Layer

Due to nature of wireless communication, openness, and sharing of physical medium, it is relatively easy for malicious nodes in the network to launch jamming radio signal to disrupt normal operation of network. Xu et al. [49] examined the radio interference attack problem and categorized four jamming attack models: constant jammer, deceptive jammer, random jammer, and reactive jammer. They further designed two schemes to detect jamming attacks by employing empirical methods based on signal strength.

At MAC layer, the randomness of random access protocols (such as IEEE 802.11 medium access control) allows misbehaving or malicious nodes to gain priority to access the shared medium after deviating their behavior from normal operation [4,24,39]. In Raya et al.'s paper [36], they found that greedy nodes making a slight modification to some parameters defined in 802.11 standard protocol could substantially increase the chance of channel occupation. The following two categories were classified: one is greedy nodes sending out selectively scrambled frames to increase victim's contention window, which gives rise to collision occurrence on victim's side that is supposed to received RTS, CTS, and ACK packets; the other is nodes manipulating protocol parameters to increase bandwidth share by transmitting after SIFS instead of DIFS, assigning large value to NAV, and reducing back-off time. A detection mechanism was designed but its effectiveness could deteriorate if its existence is known to the attacker.

Radosavac et al. [32, 33] concentrated security issues on malicious nodes choosing not to comply to standard protocol by selecting small back-off interval in order to obtain more shares of the channel over honest and normal nodes. Through modeling observation of sequence measurements of back-off interval used by malicious node, they adopt minimax robust detection approach with objective to optimize performance for the worst-case situations. Furthermore, they presented a method to decrease the number of required samples in the minimax robust detection approach. Therefore, observing node could arrive at a decision as soon as possible. Unfortunately, these techniques only work for back-off interval maneuvering attacks.

Assigning large value to Network Allocation Vector (NAV) is another way that a malicious node could use to lower channel utilization. As pointed out in Bellardo and Savage's paper [6], attackers could fabricate certain control packets with large value in duration field in order to reserve the channel for a long period of time. This is because normal nodes that received such control packets would have to update their NAV variable and be quiet. They proposed to place a limit on the duration field in order to mitigate the effect of such attacks. This would work for attacks of changing the NAV values on RTS and ACK frames, but not for CTS frame. This is because the hidden nodes from the data sender could not overhear the RTS frame and have no way of limiting the values for NAV on a subsequent CTS frame. In this paper, we present an approach to allow even hidden nodes to distinguish unsolicited CTS frames from legitimate ones, with the help of two-hop neighbor information.

Other solutions have also been investigated. Ray et al. [35] explained the false blocking problem from RTS/CTS mechanism in IEEE 802.11, which would not only propagate to entire network, but also give rise to deadlock situations. To solve this, they presented RTS validation approach to allow nodes receiving RTS packets defer a small period of time ending at the time when corresponding DATA packet is supposed to begin, instead of deferring the longer period specified in the duration field. Zhang et al. [53] studied jamming ACK attack, which has two advantages to attacker, low energy consumption for attacker and great damage to victim. The size of ACK packet is short and it consumes small amount of energy. An Extend NAV schema (ENAV) scheme was proposed to extend the ACK transmission window from T_{ACK} to $R{\cdot}T_{ACK}$, which reduces the chance of collision between normal ACK packet and fabricated ACK packet. Chen et al. [10] proposed NAV validation approach to check that a subsequent packet will be received at certain time. For instance, DATA frame should be received within $RTS\_DATAHEAD\_Time$ after RTS. Similarly, ACK frame is supposed to be received within CTS_ACK_Time after CTS packet. However, malicious nodes switching between CTS and ACK packet could avoid detection.

CHAPTER III

SCHEME DESIGN

In this section, we now elaborate on two solutions, which improve the efficiency of searching for certificate and beat the impact of CTS jamming attack respectively, and their vital parts in great details

3.1 Evidence Distribution Based on Periodic Broadcast (EDPB)

Overview

Trial pheromone is a secreted chemical substance that laid on trials by ants when they bring food back to their nest. It attracts other ants and serves as a guide to get food. As more and more ants take the same route, they too lay pheromone, further amplifying concentration of pheromone and attractiveness of the trial.

We treat this pheromone's feature as a data structure on each node in our scheme to guide query packets toward target. Similarly to the evaporation of ant's pheromone, traces should degrade as time elapses. This fits mobile networks nicely because route information could become outdated with time.

Table 1. Pheromone Evidence Table

	N_1	N_2	.....	N_m
$Cert_1$	p_{11}	p_{12}	.....	p_{1m}
$Cert_2$	p_{21}	p_{22}	.....	p_{2m}
...	...	...	.....	...
$Cert_n$	p_{n1}	p_{n2}	.....	p_{nm}

Every node stores a data structure called Pheromone Evidence Table (PET), which serves as a guide for local decision making. Each entry records pheromone concentration for a known certificate. In network routing, pheromone concentration is basically a probability value of reaching the certificate copy when the node is chosen to forward the query packet.

In Table 1, we show an exampled PET table. This node has interacted with m nodes, $N_1, N_2, \cdots N_m$ and n certificate copies have been observed. Therefore, the pheromone concentration of using node N_1 to find certificate copy 1 is p_{11}. Other pheromone concentration values have similar meanings. These values will be updated by backward ants (replying messages) and also be updated periodically to mimic the pheromone evaporation process. They will be used when a forward ant (certificate query message) tries to find a certificate copy. The details of these pheromones will be explained in Section 3.1.

Our scheme is based on ant swarm intelligence, so we try to define different types of packets as different ants. There are three types of ants: announcement ants, forward ants, and backward ants. These ants represent announcement packets, query packets, and response packets, respectively. We briefly explain these ants below. Further details will be provided in Section 3.1.

Announcement ants will travel from certificate nodes. These are actually control-flooded broadcast packets that will only travel at most TTL hops away from the senders.

Forward ants will be sent by source nodes or querying nodes, which try to find certificate copies. These packets move hop-by-hop toward the targets, looking for the requested certificate. Along the path, they will collect the identifiers of passed nodes and travel time length. Intermediate nodes with PET information toward the requested certificate will route the forward ant toward the appropriate next-hop node, but those without such information will broadcast the forward ant to all neighbors. Therefore, forward ants are capable of self-duplication which explores all potential paths toward the requested certificate.

Backward ants are returned by the certificate nodes, as replies to the forward ants. They will be routed on the path from which the corresponding forward ant traveled. Furthermore, backward ants carry the requested certificate information.

The acronyms of different ant packets are summarized in Table 2.

Table 2. Different Ant Packets

Acronym	Details
BAA	Broadcast Announcement Ant
BFA	Broadcast Forward Ant
UFA	Unicast Forward Ant
UBA	Unicast Backward Ant

Algorithm Details

Our scheme can be divided into three phases: Announcement phase, Query phase, and Response phase. While response phase usually follows query phase, the announcement phase has its own schedule that is independent of the other two phases.

Announcement Phase

In the announcement phase, the certificate nodes make periodic announcements of their existence in their neighborhood. This is the main difference of our scheme with other previously proposed schemes such as [17]. We argue that such periodic announcements update the PET table in the neighborhood of the certificate copies especially in mobile networks and allow the forward ants to find a certificate copy more efficiently.

In contrast, other schemes rely on the broadcast technique to look for certificate copy and keep track of the traces left by the backward ants. While such a technique works well in static networks, mobile networks introduce a much more difficult problem: trace invalidity. Trace can become invalid quickly in mobile networks but the trace degradation technique implemented might not be able to mimic the process accurately.

The announcement will be made in the local neighborhood of each certificate node. In particular, the announcement packets will be flooded to the TTL-hop of the neighborhood. We argue that an appropriate TTL value will allow a majority of the querying nodes to have access to updated traces. Obviously, a large TTL will generate more overhead. However, a larger TTL may not always be better even we disregard the extra cost that it introduces. This is because each certificate copy has a soft region of nodes that should contact the certificate node for certificate information. Further increasing TTL over this region size can only complicate the path selection process of the forwarding nodes. We investigate the effect of different TTL values in Section 4.1. Announcement packet also can forward to a subset of TTL-hop neighborhood, instead of flooding to all the neighbor nodes. This subset nodes will be carefully chosen by certain measures, like link quality, latency, and traffic load. Subsequently, a number of path within TTL hop region are strengthen by laying intensive pheromone. Compare to flooding announcement, this approach has lower overhead and is more efficient to locate certificate node. However, the measure that affects subset nodes selection depends on which concern the routing protocol attempts to address. We will leave this approach as future work for designing a more specific routing protocol.

The information carried by the announcement ants includes certificate identity, announcement sequence number, TTL, etc. An illustrated packet format is provided in Table 3.

Table 3. Announcement ant packet format

FIELDS	REMARKS
seq_num_	announcement sequence number
len_	packet length
src_addr_	address of announcement node
cert_id_	carrying certificate identity
last_sender_	identifier of the previous sender
hop_count_	hop count from the certificate node
ttl_	time-to-live

We propose to use the following method to estimate the best interval for announcements interval:

$$T(\sigma) = \frac{k_1}{\sigma} + k_2\alpha \tag{III.1}$$

where σ reflects mobility, α is a random number generated between 0 and 1, and k_1, k_2 are constants. For instance, k_2 can be set to 5 seconds. The estimation of σ will be discussed later. When σ is estimated accurately, more announcements will be made in high mobility networks and fewer (or just one) announcement will be made in static networks.

When announcement ants carrying certificate information is flooded to TTL-hop region, the nodes overhearing this announcement will update pheromone trace on local PET. Two updating rules can be used: one is called simple reinforcement [15] rule, defined as

$$\begin{aligned} P_i(n) &= \frac{P_i(n-1)+\Delta p}{1+\Delta p} \\ P_j(n) &= \frac{P_j(n-1)}{1+\Delta p} \qquad j \in N_k, j \neq i \end{aligned} \tag{III.2}$$

where N_k is current node's neighbor set, i is one of current node's neighbor that forwarded or sent out announcement ants. Δp is defined as $k/f(c)$ where k is a positive number constant and $f(c)$ is a non-decreasing function of cost c. Cost c could be any parameter that reveals information of certificate, such as hop count from current node to certificate node, energy consumed during transmission and available bandwidth usage of the one-hop link etc.

The other updating rule is termed advanced reinforcement rule, which proportionally distribute current node's pheromone evidence to its neighbor node, according to trust evidence metric ($M_{i,k}$). $M_{i,k}$ could be any metric measurement among the current node and one of its neighbors, such as energy consumed, traffic load experienced, and distance etc.

$$P_i = P_k \cdot \frac{M_{i,k}}{\sum\limits_{j \in N_k} M_{j,k}} \tag{III.3}$$

where j is current node, and i is one of node j's neighbor [15, 17].

Query Phase

A node requesting for a certificate copy initiates a query phase, in which a forward ant is sent and intermediate nodes help to route the forward ant toward a certificate copy.

The difference of regular packet routing and query phase is the self-duplication of forward ants. We define two kinds of forward ants: Broadcast Forward Ants (BFAs) and Unicast Forward Ants (UFAs). When a node receives a forward ant (be it a BFA or a UFA), it will look at its PET table and decide whether to send out a BFA or a UFA. Furthermore, if a UFA is to be sent, the receiver of the UFA will be chosen based on the PET table stored on the sending node.

When a sending node cannot find any immediate neighbor with positive trace toward the queried certificate copy, a BFA will be sent. Therefore, all immediate neighbors will receive a copy of the forward ant (to process/forward). However, if there exists at least one immediate neighbor with positive trace toward the queried certificate, a UFA will be sent and the immediate neighbor with the highest pheromone value on the PET table will be chosen to be the receiver of the UFA.

The logic behind such a strategy is rather straightforward: when no neighbors know about the certificate copy, the sending node has no other choice but to send it to every neighbor. When one or more neighbors have traces toward the certificate copy, the neighbor with highest trace (pheromone) should be chosen to forward the query message (the forward ant). It is this simply decision making based on PET (local information) that leads to nodes behavior coordinately. Eventually, these cohesively individual behaviors achieve global common goal that deliveries BFAs and UFAs to the requested certificate.

In addition, forward ants always carry the identifiers of the nodes that they pass through. These information will be needed in the response phase, which is in charge of sending the certificate information back to the querying node. However, information carried on forward ants is not subject to identifiers of traversed node, it can be a broad variety of information categories which depends on what concerns emphasized on in designing routing protocol. For example, goodness value of link [12] and delay contained in forward ants are designed for a routing protocol that could balance network load; energy consumption and latency information carried [16] on forward ants is for a both energy critical and latency critical network.

Care must be taken to remove forward ants running the network endlessly, either through a loop or some mis-routes. In order to ensure this behavior, a TTL value is inserted in each forward ant generated by the querying node. Every node processing a received forward ant will decrement the TTL value. When TTL reaches 0, the forward ant will be purged from the network. Another approach to prevent loops is detecting loop in the chain of identifiers of traversed nodes forward ant collected. Compare to TTL approach, this approach is more accurate, but requires more computing resources and times. Consider the limitation of resources, CPU speed and memory size in sensor node and latency is one of performance metrics we will investigate in section 4.1, we choose the TTL approach to prevent loops.

Response Phase

Once a forward ant reaches a certificate node, the response phase will be initiated. In particular, a backward ant will be generated and sent back to the querying node.

There are two issues worth of discussion: the backward ant will use the information stored on the arriving forward ant; there might be more than one forward ant arriving at the node carrying a certificate copy. Information collected from identifiers of intermediate nodes is usually used to allow backward ant travel back to source node along exactly same path as the original one. Other performance metrics information memorized on forward ants, like latency, energy and link quality is a critical factor for certificate node to release backward ant for certain arriving forward ants. There are some strategies that certificate node can choose for sending out a number of backward ants. Certificate node could replay with a backward ant for every each arriving forward ant or release top-k backward ants with respect to certain performance metrics by comparing all the arriving forward ants. In this work, the number of response backward ant is same as the number of arrived forward ants since we argue that every path could be a good quality path in a volatile context network.

In addition, each intermediate node will update its PET table using reinforcement rules concerning the certificate copy and the node from which it receives the backward ant. Similarly to the PET update in the announcement phase, two reinforcement rules can be designed: one is simple reinforcement rule for fixed network that has been discussed in the announcement phase; the other being the advanced reinforcement rule proposed in [17] for mobile network, defined as:

$$P_i(t) = \frac{[\tau_i(t)]^\alpha [\eta]^\beta}{\sum\limits_{j \in N} [\tau_j(t)]^\alpha [\eta_j]^\beta} \tag{III.4}$$

where η_i is the goodness value of the link between current node k and its neighbor node j. α and β are constants varied in different network environments and determined usually by simulation. τ_i is the pheromone deposit, which is first defined in [17]:

$$\begin{aligned} \tau_i(t + \Delta t) &= f(\tau_i(t), \Delta t) + \Delta p \\ \tau_j(t + \Delta t) &= f(\tau_j(t), \Delta t) \qquad j \in N, j \neq i \end{aligned} \tag{III.5}$$

where Δp is the same as in (III.2). $f(\tau_i(t), \Delta t)$ is the pheromone evaporation function defined as [17]

$$f(\tau_i(t), \Delta t) = \tau_i(t) \cdot e^{-\Delta t \cdot \sigma / k} \tag{III.6}$$

where σ is the same as in (III.1).

Equation (III.4) presents the formula for emulating the real pheromone evaporation by making the pheromone evaporate over time to reduce the probability that the packet forwards to outdated trails in mobile network. The speed of pheromone evaporation is dynamically changed according to node's mobility by mobility statistics which records a set of mobility measures in a observation window. Node could also dynamically make a switch between these two reinforcement rules by calculating σ value out. A threshold value for σ, e.g. 0.2, in our simulation, could represent the threshold to decide whether it is a static or mobile network.

3.2 Addressing inspection schema (AIS)

In this section, we introduce a countermeasure called address inspection schema (AIS) to mitigate the effect of CTS jamming attack.

Overview

First of all, we declare several notations that will be used throughout this work. We define N_k as the neighbor set of node k. Furthermore, we use N'_k to represent the two-hop neighbor set of node k, which can be computed by the union of neighbor sets of node k's neighbor nodes. So, $N'_k = \bigcup_{j \in N_k} N_j$.

The main idea of our AIS technique is to check the targeting address carried on the CTS packets. With the help of two-hop neighborhood information, nodes can decide whether the targeting address of a CTS packet is legitimate. This is because, except in dynamic networks, all overheard CTS packets should have targeting addresses that belong to the two-hop neighborhood set. This is true for each of the neighbors of the CTS packet sender. The decision-making procedure for each node receiving or overhearing CTS packet has the following phases:

Prerequisite phase: Node k sends out HELLO message carrying N_k to all its neighbors so that other nodes can obtain their neighborhood information. This phase should be performed periodically. It is important to ensure the freshness of N'_k.

Inspection phase: Node k inspects targeting address specified in the RA (Receiver Address) field of CTS packet. One of the following scenarios may arise

- **I1:** the targeting address is k and node k has sent an RTS packet. The CTS packet is obviously legitimate. Node k proceeds with the normal operation;

- **I2:** the targeting address is k and node k has not sent an RTS packet. The CTS packet is obviously illegitimate. Node k proceeds with the Clearance phase below;

- **I3:** the targeting address is not k and it belongs to the set N'_k. The CTS packet could be legitimate. Node k proceeds with the normal operation, i.e., updating NAV;

- **I4:** the targeting address is not k and it does not belong to the set N'_k. The CTS packet is illegitimate. Node k ignores the CTS packet.

Clearance phase: In this phase, node k sends out a control packet, termed Clear Reservation (CR), to instruct neighbor nodes to ignore the channel reservation from previous CTS control packet. All nodes overhearing a CR message should ignore the CTS packet, recover the original NAV value.

In order to be able to recover the original NAV value after fabricated CTS attack detection, nodes overhearing CTS messages should not simply update their NAV values right away. Instead, they should keep a copy of the FCS of the CTS message and record the current NAV value before updating it. When a CR message is overheard, they will use these information to look for NAV value to recover.

Table 4. Packet format of the clear reservation control packet.

FIELDS	BYTE	REMARKS
frame control	2	control fields
TA	6	source address
FCS'	4	FCS of the suspected CTS packet
FCS	4	FCS of this message

The information carried by CR packet includes frame control, identification of previous CTS packet, source address, etc. Frame control field has the same structure as illustrated in IEEE 802.11 specification, except one new value is introduced for subtype field, CCTS, meaning clear previous CTS packet's reservation. The FCS' field is copied from the FCS field in the fabricated CTS packet. This functions as identification for the detected fabricated CTS message. A detailed CR packet format is provided in Table 4.

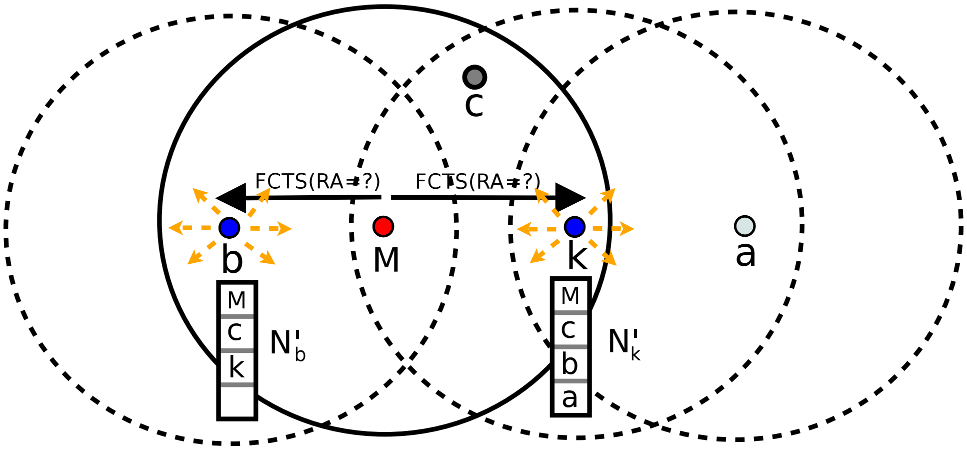

Figure 1. A scenario illustrating fabricated CTS jamming detection. The network is consisted of five nodes, a, b, c, k, and M. Node M is a malicious node sending out CTS jamming packets randomly. If the targeting address of the fabricated CTS packet from node M is a node outside of this neighborhood, e.g., node x, nodes b, c, and k will detect the jamming and ignore the CTS packet. If node M sends a fabricated CTS targeting at node k, then node k detects it and broadcasts a CR message to notify node c (note that node b is still suffered from the attack). If node M sends a fabricated message to node a, node b detects it and ignores the CTS message (note that node k cannot detect the jamming message).

An illustrative example is provided in Fig. 1. Under different attack methods, the neighboring nodes, if not all, will detect such fabricated CTS messages and clear the channel reservation.

Detection Analysis

We have the following analysis regarding to the AIS operation.

Incomplete Detection: As can be seen from the previous discussions, under some attacks, only some neighbors will detect the attack and ignore the fabricated CTS message. Other nodes will still be forced to be silent. This should not have significant impacts on the throughput recovery of the AIS scheme: with some of the nodes in the neighborhood ignoring the fabricated CTS message, they are free to send out channel request or data transmission, occupying the channel instead wasting it for idle. This beats the purpose of the attack.

Communication Overhead: There are two types of additional/revised packets that need to be transmitted: HELLO messages containing each node's neighbor list and the CR message. The HELLO messages are usually broadcast periodically even without the AIS scheme. We only modify the HELLO message to include the neighbor list of the message sender, so that the neighbors can gather information about two-hop neighbors. Note that such information may require some time to obtain.

The CR message will be sent by the node whose ID serves as the targeting address on the fabricated CTS packets. This message is only sent when the node is under attack. As we explained in the Introduction section, we assume that fabricating source address is difficult for attacker (with radio fingerprinting technique in place [14]). Only the node with ID as the targeting address on a suspected CTS message can send a CR message.

CHAPTER IV

EXPERIMENTATION AND EVALUATION

To avoid interaction of performance of two schemes, this section evaluates each of them by setting separate environment.

4.1 EDPB Experiment

Experiment Setup

In order to study the characteristics and evaluate the performance of EDPB, we have set up simulation experiment using NS2. A total of $N = 300$ nodes are uniformly distributed in a field of 3000 × 3000 meters. The transmission range is 250 meters and the data rate of the wireless channel is 2 Mbps. Our experiment proceeds in rounds. In the beginning, several nodes are randomly selected to carry the certificate. Then some other nodes are chosen to request the certificate information. All results are the average of 20 runs.

We simulate two types of networks, static and mobile networks. In static networks, nodes never move. In mobile networks, however, the nodes move at a speed randomly chosen from 0 to a maximum speed, V.

Performance Metrics

Our evaluations focus on two major metrics: cost and latency. Cost is defined as the total number of ant packets transmitted due to each certificate query. Since packet transmission is proportional to energy consumption, such a cost also represents the energy cost to query the certificate. The second major metric that we will investigate is latency. Latency is defined as the elapsed period between the time when a querying node sends out the query and the time when the result comes back.

We placed λ copies of the same certificate in the network and querying nodes send their requests subsequently looking for a certificate node. More advanced cache placement techniques can be used [28], but are considered out of the scope of this work. Unless specified otherwise, our simulations were based on the following parameters. 10 queries from different nodes are sent in each simulation. All simulation results are the average of 20 runs with different seeds.

In mobile networks, we further investigate success ratio, defined as the number of queries that actually find a certificate node divided by the total number of queries. This metric represents the robustness of an evidence distribution scheme against network dynamics. Another metric that we investigate is redundancy, measured as the number of backward ants that each query triggers. As mentioned in section 3.1 and 3.1, one forward ant could duplicate itself as it searches toward the certificate node. Therefore, more than one forward ant in the same query may reach the certificate node eventually, triggering multiple backward ants. Such a measurement can represent the unnecessary cost for a query.

Static Networks

We first investigate the cost of ant packets transmitted in static networks. The simple reinforcement rule (see (III.2)) is employed in both the announcement phase and response phase. $k = 0.5$ and $f(c)$ is defined as the number of hops from the certificate node.

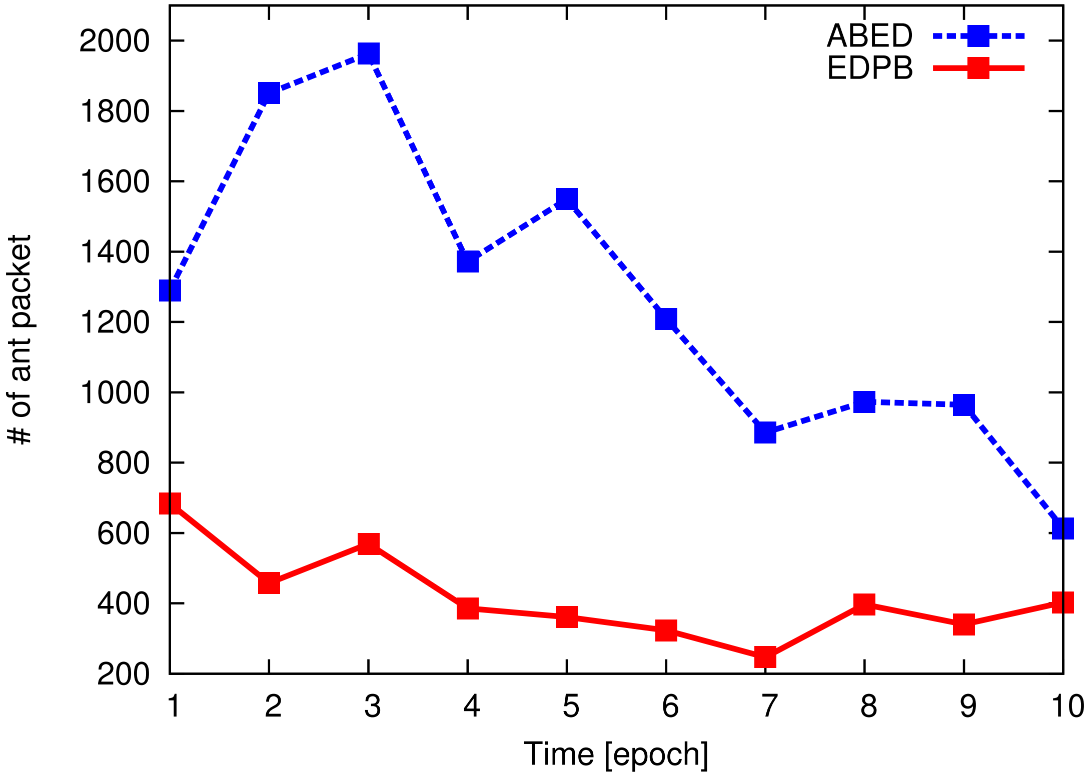

Figure 2. The total number of ant packets, N_a, which includes forward ants (BFA and UFA), backward ants, and announcement ants (in our EDPB scheme). We compared N_a of ABED and EDPB in static networks. The N_a value of EDPB is consistently lower than that of ABED.

The total number of ant packets, N_a, is presented in Fig. 2. There is $\lambda = 1$ certificate node randomly placed in the network. We showed the results as a function of time. In particular, we defined epoch as the interval in which one query is sent. As can be observed in Fig. 2, EDPB has much lower N_a values than ABED. This is a direct result from the announcement phase, which announces the topological location of the certificate nodes. Such information avoids the costly transmission of BFAs, which will be sent when the sender has no preferred forwarding node.

The overall trend of N_a as a function of time is decreasing over time. This can be explained by the additional traces left by the backward ants. Hence all later queries are more likely to take advantage of these traces and avoid sending BFAs. There is a surprising upward trend in ABED's N_a numbers in the first three queries. These might have been caused by the training nature of the first few queries in swarm intelligence.

In order to investigate the effect of leaving traces (pheromone) on nodes' PETs, we investigated and compared the numbers of different ants being transmitted in the EDPB scheme in a simulation of 200 seconds with 100 queries sent from randomly chosen nodes.

Figure 3 presents our simulation results on the numbers of different types of ants. As expected, the number of BAAs remains the same throughout the simulated period, confirming the strategy of periodic announcement from the certificate nodes. It is more interesting to compare the numbers of BFAs and UFAs. Our first observation is that the number of UFAs are much higher than the number of BFAs, meaning that more query packets are sent as unicast instead of being broadcasted. This is due to the periodic broadcast announcements from the certificate nodes. As a number of reference, the number of UFAs is about 3 times as large as that of BFAs. The second observation between the numbers of BFAs and UFAs is that they both decrease as time passes on, except for a bump in the number of UFAs around 80 seconds. The bump might have been caused by some unfortunate querying nodes. The overall decreasing trend confirms that the traces from UBAs and BAAs are working.

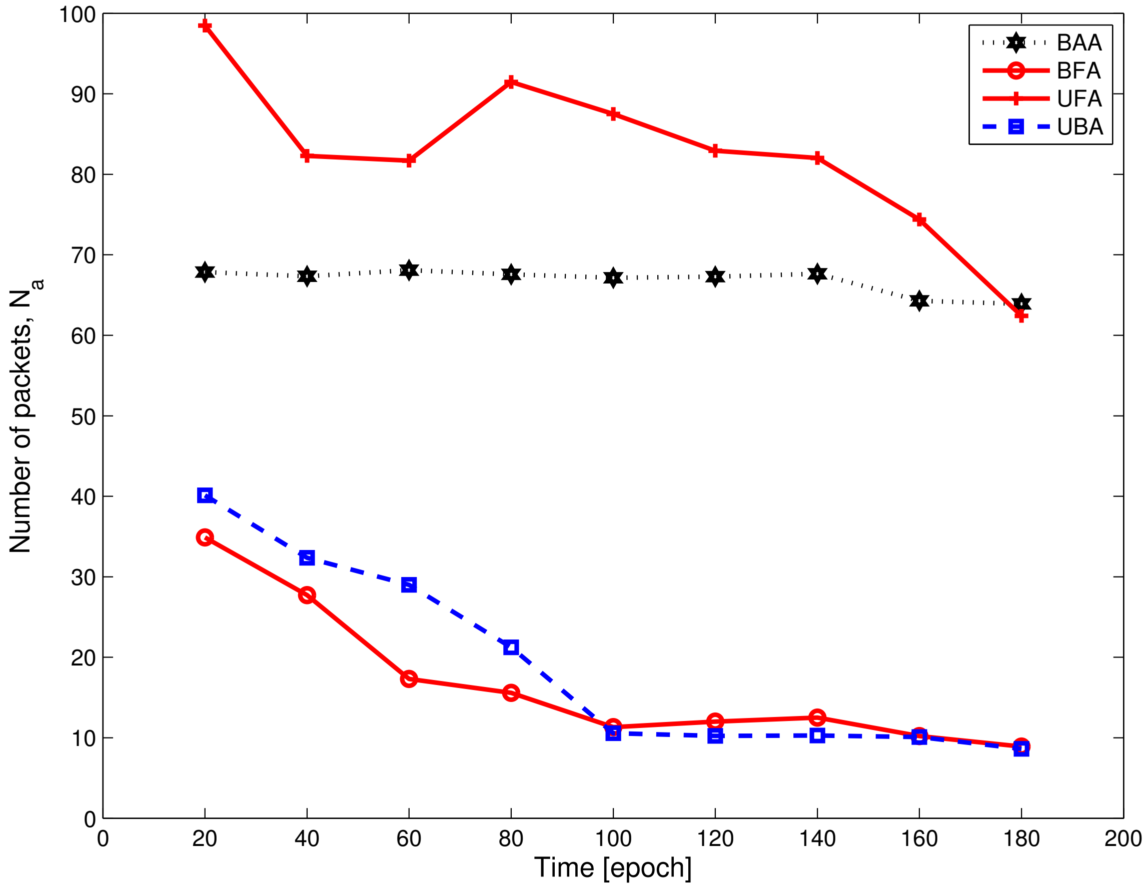

Figure 3. The number of different ant packets, BAA, BFA, UFA, and UBA. We want to observe the change of different ants being sent in the network as time goes on (with more and more traces or pheromone left on the PETs).

The number of UBAs is roughly the same as the number of BFAs, with a similar decreasing trend as time passes on. Therefore, as more and more queries are being sent and processed throughout the network, the PETs tables are collecting traces toward the certificate nodes. Hence, fewer and fewer forward ants will reach the certificate nodes and fewer number of backward ants will be sent back as responses.

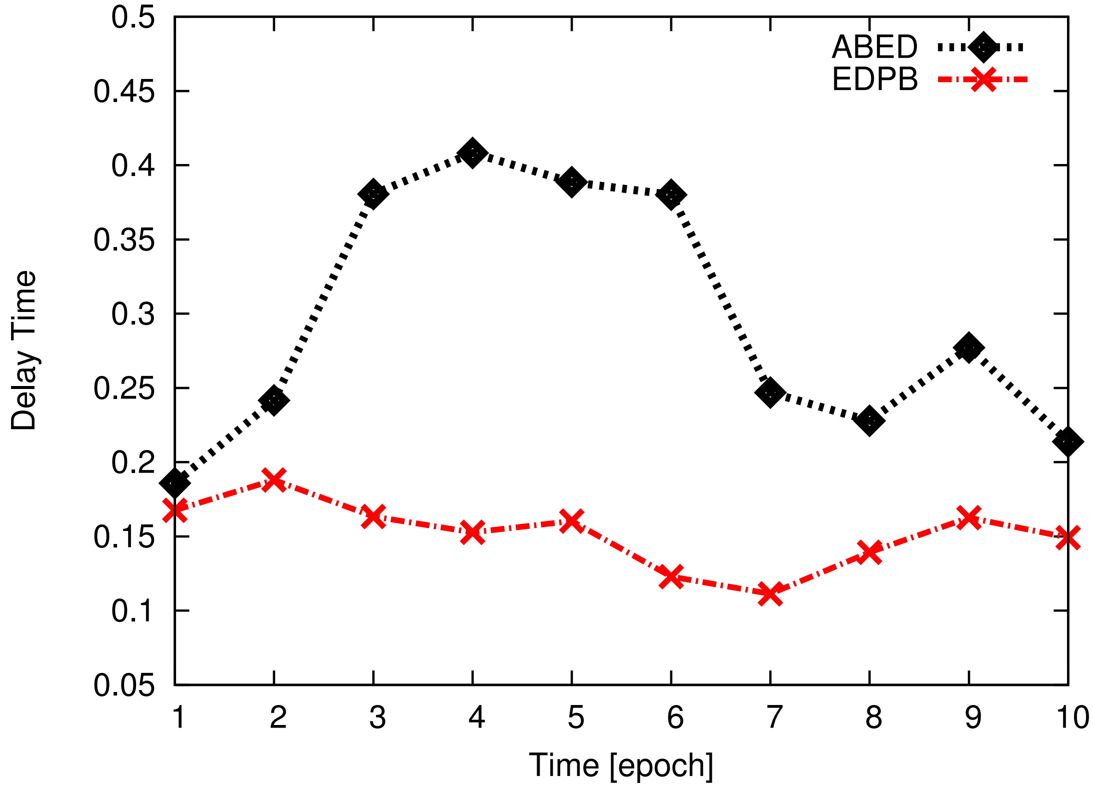

Figure 4. Query delays, T, of the ABED and EDPB schemes in static networks. The query delay is defined as the overall time that a query spent in the network. Neglecting the processing delays at the querying node and the certificate node, T is the sum of forward ant travel time and UBA travel time in the network. We can see that the query delay of the EDPB scheme is lower than that of the ABED scheme.

We further investigated query delay, T, of the ABED and EDPB schemes in static networks. The network setup is similar to that of Fig. 3. The query delay is defined as the overall time that a query spent in the network. Neglecting the processing delays at the querying node and the certificate node, T is the sum of forward ant travel time and UBA travel time in the network. As can be seen from Fig. 4, the query delay of the EDPB scheme remains at 0.15 second for all the queries that we tested. The query delay of the ABED scheme, however, fluctuates a lot as the numbers of BFAs and UFAs change between different queries. The initial increase of query delays in the ABED scheme might have been caused by more and more ant packets being transmitted in the network. Subsequently, as more and more traces are stored on PET tables, the query delay is shorter.

Mobile Networks

Node mobility could quickly invalidate the pheromone trace on PET tables. However, with the help from our periodic announcements, the PET tables will remain accurate and allow forward ants to locate certificate nodes quickly. We evaluated our scheme and the ABED scheme in different mobile networks in this section.

Our simulations used periodic announcements in (III.1), with $a = 1$ and $\sigma = 0.5$, which is proportional to actually mobility. We borrowed the concept of σ from Subramanian et al. in [43]. In their mobility statistics, σ is the variance of trip times. In our implementation, we estimate the trip times as the transmission delays for forward and backward ants over a moving observation window. The advanced reinforcement rule is used when backward ants are received, as defined in (III.4). $\alpha = 1$ and $\beta = 2$, and σ is set to 0.5. The announcement ants will still be processed with the simple reinforcement rule. We leave the further investigation of these reinforcement rules as future work.

The success ratios of the ABED and the EDPB schemes are compared in Fig. 5, under various mobility. The mobility is demonstrated with the maximum speed from which each node chooses its actual speed of movement. From this figure, we can see that the ABED scheme has a quickly degrading success ratio as network mobility increases. For example, when the maximum speed is 15 m/s, the success ratio of the ABED scheme is about 0.1. On the other hand, the EDPB scheme enjoys high success ratio even under high mobility. Note that the success ratio of 0.9 in low mobility network could be due to a response timeout in the first query.

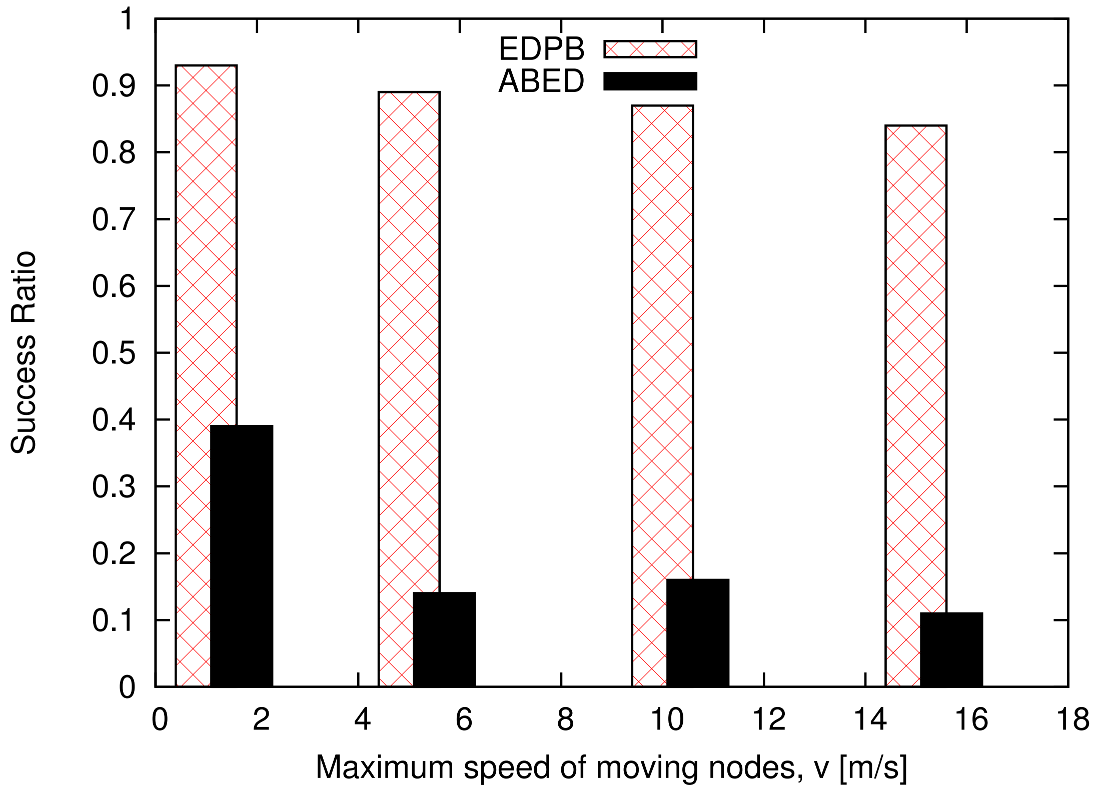

Figure 5. Success ratio of the ABED and the EDPB schemes. Success ratio is defined as the ratio between the number of queries that eventually locate certificate nodes and the total number of queries. The ABED scheme suffers from the low success ratio problem. On the other hand, the EDPB scheme maintains a success ratio of 0.8 and 0.9 even under high mobility.

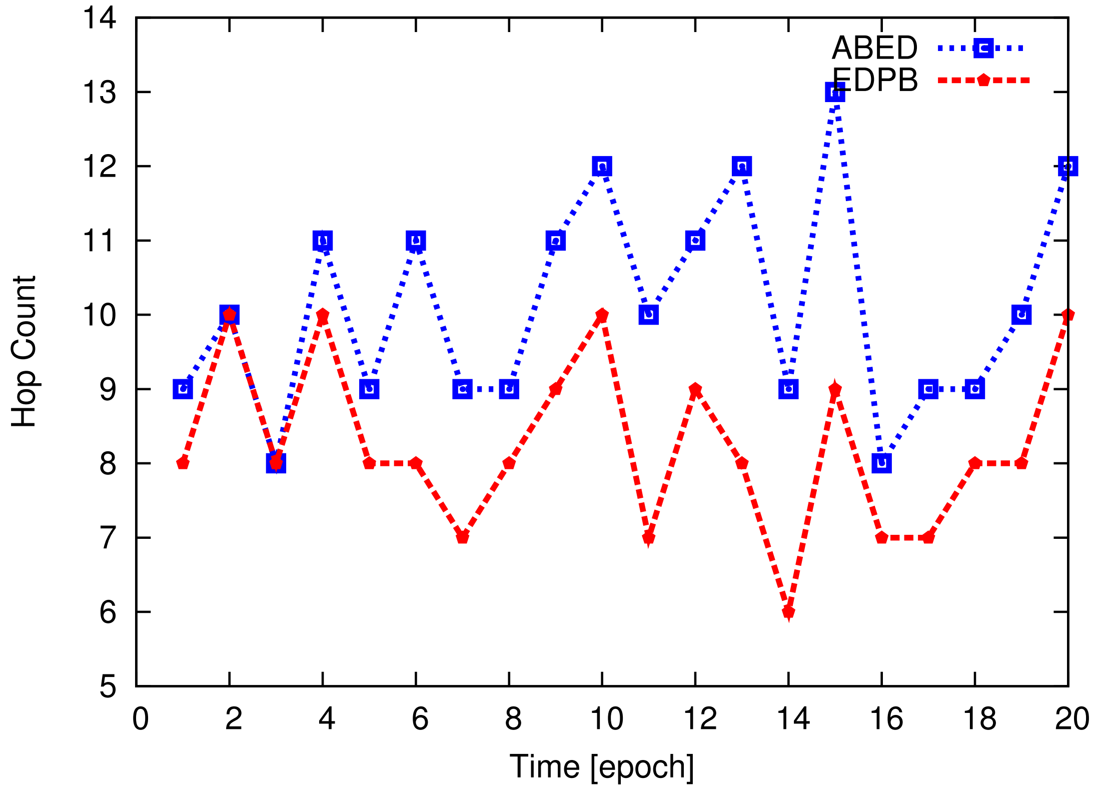

Figure 6. Hop-count comparison of the ABED and EDPB schemes in mobile networks. We measured the hop-counts that each of the response packets traveled. This represents the scheme's capability of finding the shortest path between the querying node and the closest certificate node.

In Fig. 6, we compared the hop-count that each of the response packets (backward ants) traveled. Such a value represents the quality of the identified paths. The EDPB scheme offers better hop-count than the ABED scheme, even though some fluctuations can be observed. The gap between EDPB line and ABED line shows that our EDPB scheme can find the shorter path than ABED scheme does. The reason behind this is pheromone laid by announcement packets significantly leads forward ant that arrives at the edge of announcement area to find the shortest path to certificate node, whereas forward ants in ABED have to explore possible paths in which detour path exists.

In Fig. 7, we compared the delay performance of the ABED and EDPB schemes. The simulation setup was similar to that of Fig. 4. Nodes moved at a speed randomly chosen from 0 to 2 m/s. We only measured the shortest delay for each query. We can see that the EDPB scheme has consistently shorter delay than the ABED scheme. In fact, the EDPB scheme enjoys a short delay of about 0.1 second, but the ABED scheme has up to seconds of delay. This is because of the additional transmissions in the ABED scheme, searching for the certificate copies. The extra delay could have also been caused by the outdated trace on PETs that lead the forward ants toward the wrong location. Once the forward ants reach the location, they will have to be re-routed in search of the certificate nodes, causing more collisions and delay.

In Figure 8, we compared the redundancy of the ABED and the EDPB schemes. The redundancy represents the overall number of backward ants returning to the querying node in each query. We can observe that the EDPB scheme has lower redundancy as compared to the ABED scheme. The fluctuation of redundancy in the ABED scheme can be explained by the sometimes lack of valid trace toward the certificate nodes at some locations. The broadcast announcement in the EDPB scheme allows the nodes in the neighborhood of the certificate nodes to store valid traces toward them.

To further evaluate the EDPB scheme, we have investigated its delay performance under different broadcast announcement intervals. The results are shown in Fig. 9. As the announcement interval increases, the delay increases. This is expected: with longer announcement intervals, fewer announcements are made, making the traces on the PET tables less accurate. An extreme case is to use an very long announcement interval in mobile network, representing the EDPB with just one or no announcements.

4.2 AIS Experiment

Experiment Setup

order to study the characteristics and evaluate the performance of AIS, we set up simulation experiments using NS2. The wireless transmission range is 250 meters. One node is put into the network serving as the attacker which would periodically send out CTS jamming packets.

We simulated two different types of attacking strategies for the attacker: one targets at non-existing node address, which is termed as “Blind Fabricated CTS” or “Blind FCTS”; the other targets at random node address, which is termed “Focus Fabricated CTS”, or “Focus FCTS”.

Then, we carried out simulation for the following four scenarios.

- **normal**: network under no FCTS attacks and the AIS;
- **Blind FCTS**: network under Blind FCTS attacks but without AIS running;

- **Blind FCTS + AIS**: network under Blind FCTS attacks and AIS is running;
- **Focus FCTS + AIS**: network under Focus FCTS attacks and AIS is running.

Unless specified otherwise, all remaining parameters used in simulations are listed in Table 5. The attack period is the duration for each FCTS packet and the attack interval is the interval between two consecutive attacks.

Table 5. Simulation Parameters

Simulation	25 sec.	Routing Protocol	AODV
Attack Start Time	8th sec.	AIS Start Time	13th sec
Attack Period	6 msec.	Attack Interval	7 msec.
CBR data rate	120Kb	CBR packet size	100 bytes

Performance Metrics

Our evaluations focus on two major metrics: throughput and delivery ratio. Throughput is defined as the total traffic transmitted in network. Throughput can be considered as the indicator of network functionality. Note that the throughput presented here is the so-called "instant throughput", which measures the instantaneous throughput, or the number of bits transmitted/received successfully in a unit time.

The second major metric that we investigate is delivery ratio, defined as the number of received packets at the receiver divided by the number of transmitted packets. This represents the success ratio of actual transmission.

Performance Evaluation

We first present the results of a pre-assigned network, in which a total of $N = 12$ regular nodes are placed in a field of a 500 × 500 meters. The attacker locates at the center of the network. As Fig. 10 shows, without attacker in network, the data transmission is stable, and overall trend of transmission stays at a horizontal level. However, when the Blind FCTS attack is introduced, throughput drops to almost 0, starting from the 8th second, which is the attack starting time. This is because the sender is forced to be silent after the Blind FCTS attack.

However, with the help from AIS, victim nodes would ignore illegitimate channel reservation from the attacker, this is demonstrated by two curves in Fig. 10, "Blind FCTS + AIS" and "Focus FCTS + AIS". After the AIS scheme is activated at 13th second, the throughput curves quickly climb up and approach stable throughput. For Blind FCTS attacks, AIS allows every node to detect such attacks and ignore the corresponding NAV reservations. Based on Fig. 10, the last part of "Blind FCTS + AIS" curve is very close to the curve of the normal network, showing that the network has recovered the throughput to original level.

For Focus FCTS attacks, AIS could only recover a majority of the throughput since attacker alternated targeting address randomly. This could be observed in Fig. 10, i.e., the gap in the stable throughput region between "Focus FCTS + AIS" curve and "Blind FCTS + AIS" curve. The reason for such a gap is the detection failure by the AIS scheme (such as the failed detection by node k when node M sends an FCTS message to node a). In addition, we could observe that the lowest point of "Focus FCTS + AIS" curve is around 20, which is different from that of "Blind FCTS + AIS" scenario. The protection described in IEEE 802.11 standard could explain such a phenomenon: when a node receives unexpected CTS packet targeting to itself, it will discard this packet and is free to use the channel later on.

We also simulated our scheme in a network where $N = 40$ nodes are placed randomly in a region of 1200×1200. We selected more sender-receiver pairs in order to observe the effect of attack and AIS in a network with higher traffic load.

In Fig. 11, we present delivery ratio results in normal, Blind FCTS only, Blind FCTS plus AIS and Focus FCTS plus AIS networks. The results were obtained through stable conditions, i.e., no dynamic behavior by the attacker or AIS during the observing window. In normal network, overall trend of delivery ratio stays at a high level, and drops slightly at the end, caused by the heavy traffic load. Delivery ratio in Blind FCTS only network is about 0.22 with low traffic load. Seemingly surprisingly, it rises to 0.28 as the traffic load increases. This can actually be explained by the additional pairs of communications, some of which might not be jammed by the attacker.

Networks with AIS running maintain a high delivery ratio, dropping slightly with heavy traffic load. This shows that the use of the AIS technique allows nodes to detect the FCTS attacks and are free to use the channel.

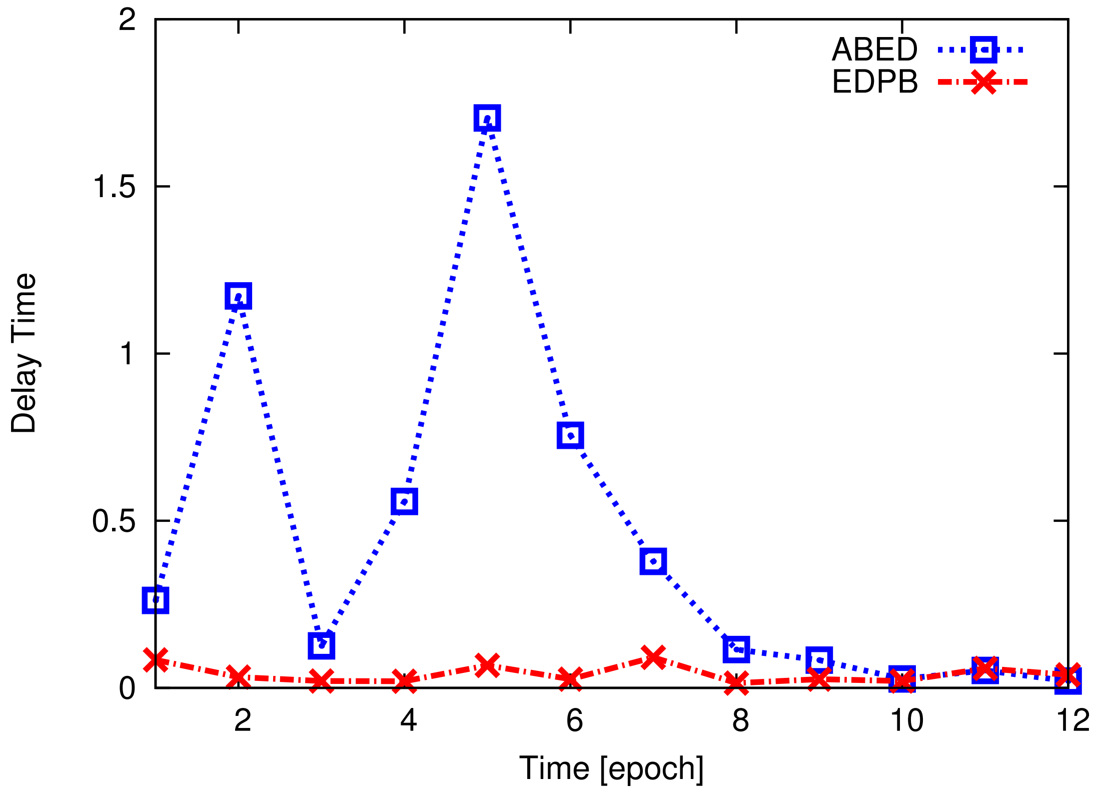

Figure 7. Delay comparison of the ABED and the EDPB schemes in mobile networks. The nodes move at a speed randomly chosen between 0 and 2 m/s. We measure the delay as the time when the querying node sent out the forward ant and the time when the backward ant returns. It can be seen that the EDPB scheme offers much lower and consistent delay than the ABED scheme does.

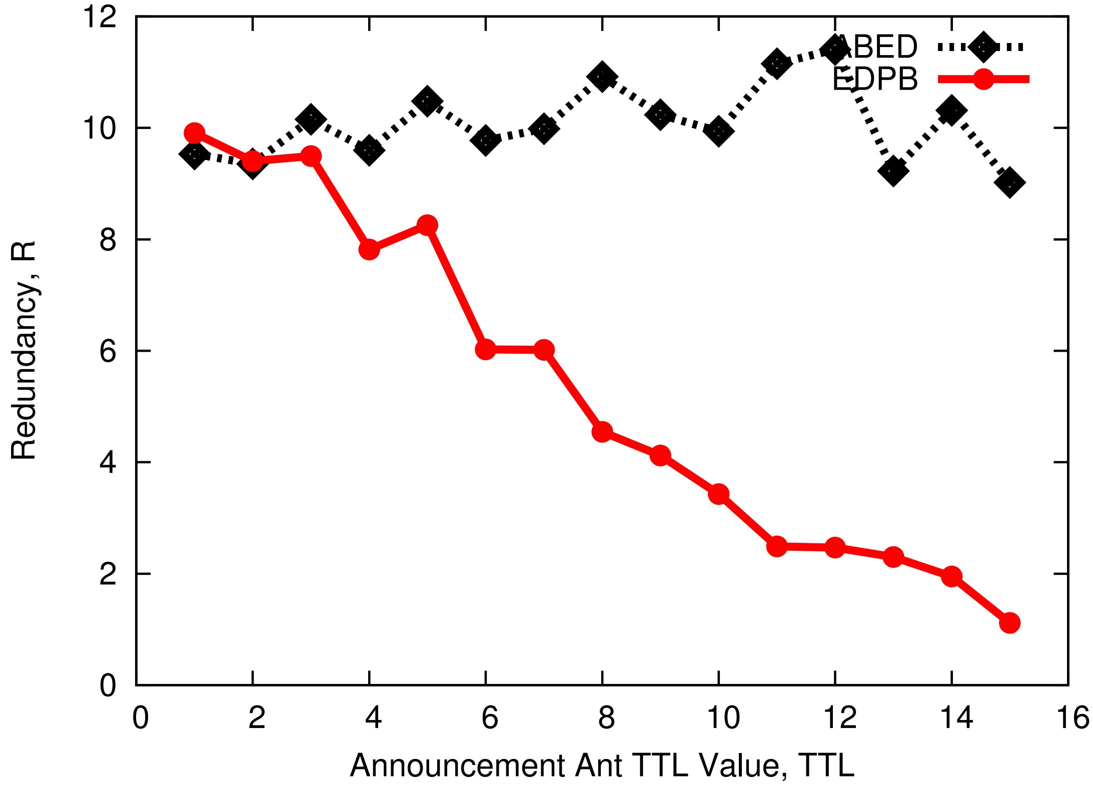

Figure 8. Redundancy comparison between the ABED and the EDPB schemes in mobile networks. Redundancy is defined as the number of backward ants returning to each of the query packet (or forward ant sent by the querying node). This performance metric represents the overall redundancy or unnecessary transmission in the network when nodes are searching for certificate nodes. The optimum value should be 1 but in practice, it can take values higher than 1.

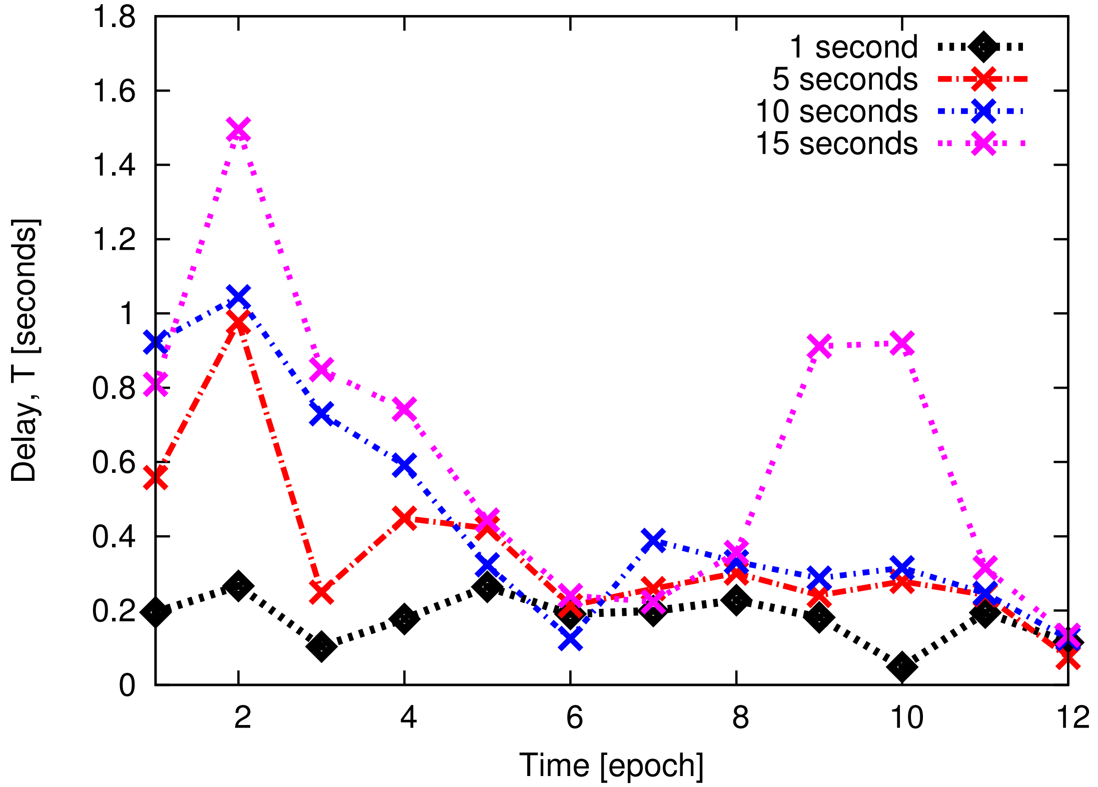

Figure 9. Delay performance of the EDPB scheme under different broadcast announcement intervals. The different legends represent such different intervals. It can be seen that the delay generally increases with the interval.

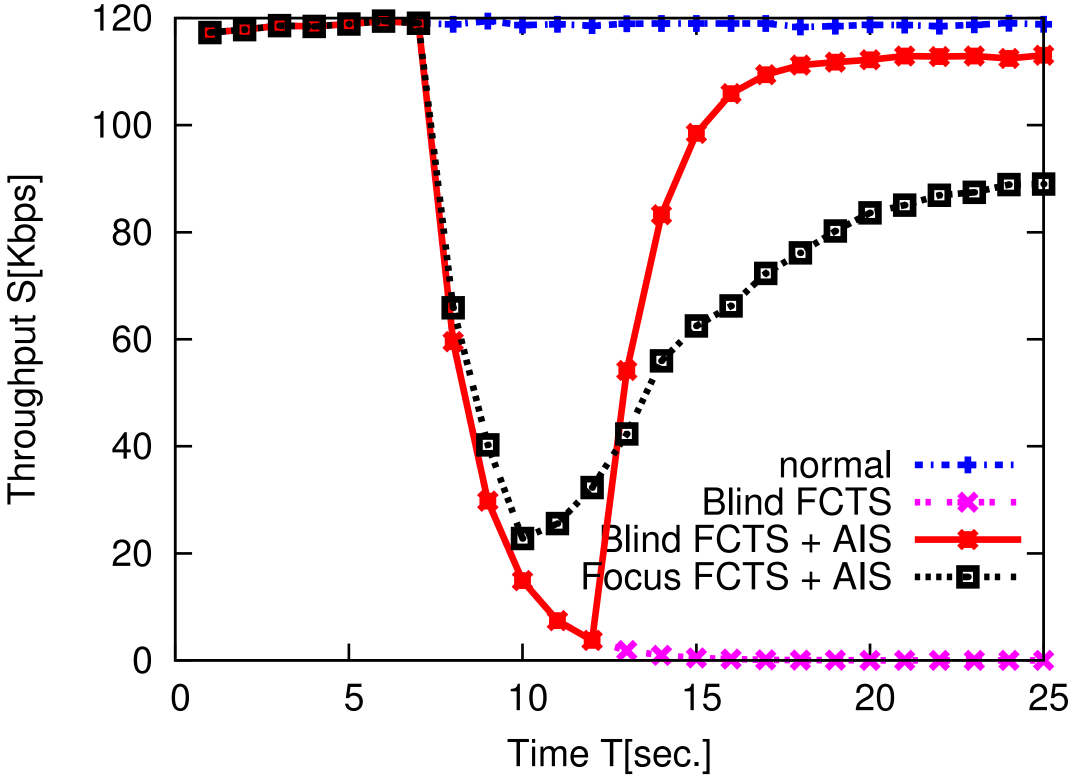

Figure 10. Throughput performance in normal, Blind FCTS only, Blind FCTS plus AIS and Focus FCTS plus AIS networks. Jamming attack starts at 8th second. AIS kicks in at 13th second. As we can see, AIS helps network to restore most portion of original transmission when network is under attack.

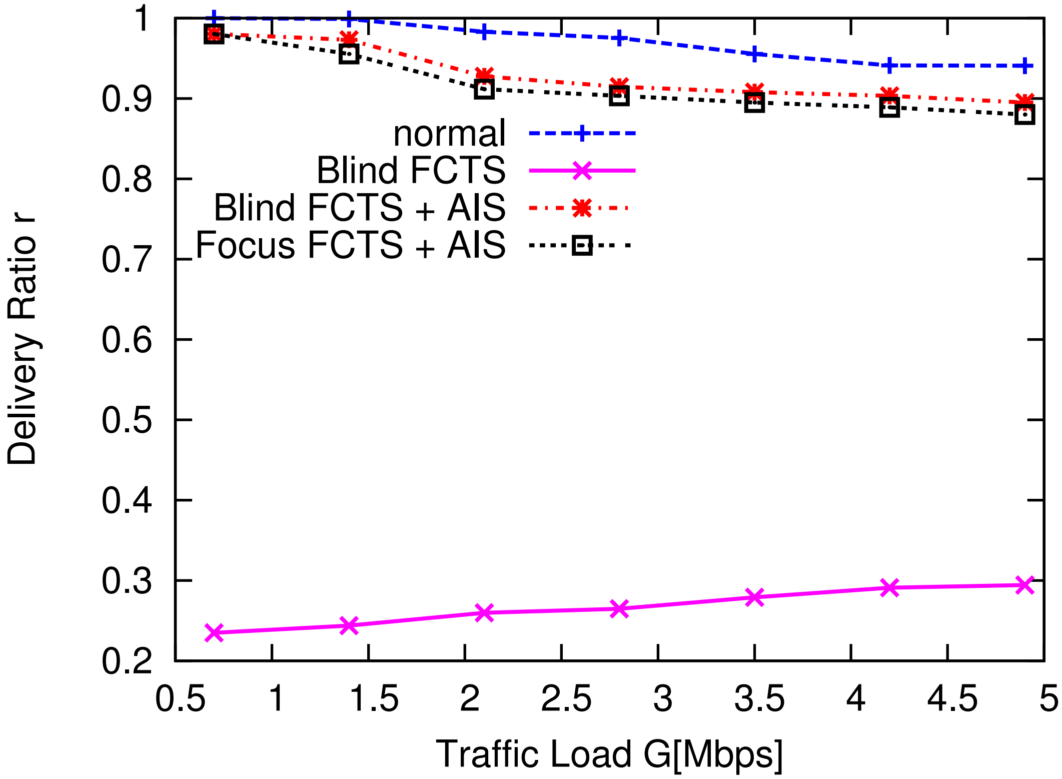

Figure 11. Delivery ratio comparison in normal, Blind FCTS only, Blind FCTS plus AIS and Focus FCTS plus AIS networks as traffic load increased.

CHAPTER V

CONCLUSIONS AND FUTURE WORKS

In an asymmetric cryptography wireless network, it is a huge challenge for nodes to search for trust certificate efficiently while the network is exposed to attacks violating IEEE 802.11 standard. In this work, we have investigated two of these problems and proposed two effective solutions, Evidence Distribution based on Periodic Broadcast (EDPB) and address inspection schema (AIS).

EDPB allows querying nodes to locate requested information more quickly and efficiently both in static and dynamic network. EDPB not only takes advantages inherited from swarm intelligence, such as local information possession that does not cause extra overhead of interaction with environment and lowered transmission number in network, but also makes essential announcements that leave trace information on those potentially optimal paths which can yield better performance in cost and delay. This scheme can be used for data dissemination and query in other mobile wireless networks such as vehicular networks. Instead of searching for certificate, other essential data or information can be queried.

In the future, EDPB can be improved by comparison with other state-of-the-art schemes and be implemented it on mobile devices for field tests. Theoretical analysis of the optimum TTL and pheromone update rules can be beneficial as well.

AIS helps nodes distinguish legitimate CTS packets from fabricated ones by using the help of tow-hop neighborhood information and inspecting the targeting address on the CTS packet. When such targeting address falls within the two-hop neighborhood of the attacker, some nodes in the network will be able to detect the attack and ignore the illegitimate claim of channel reservation. AIS simulations showed that jamming attack could be easily distinguished, and a significant portion of network throughput can be recovered.

In our future work, we will investigate the jamming attack in mobile networks and evaluate the performance of our proposed scheme in such networks. An approach of delayed action can be used: only after detecting a fabricated CTS message a few times will a node ignore the NAV value from the message. This will provide extra protection for communication of mobile nodes. Theoretical analysis of the performance of our scheme will be performed as well. Furthermore, the overhead of two-hop neighborhood information will be investigated in different networks.

At the final step of future work, we will combine these two solutions in a complex scenario so that distributed trust evidence can be searched with low cost and delay while the effects of CTS jamming attack can be mitigated.

REFERENCES

[1] IEEE standard for wireless LAN medium access control and physical layer specifications, p802.11. 2007.

[2] A. Abdul-Rahman and S. Hailes. A distributed trust model. *portal.acm.org*, 1998.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38, 2001.

[4] B. Awerbuch, R. Curtmola, D. Holmer, and C. Nita. Odsbr: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. *ACM Transactions on Information and System Security (TISSEC)*, Jan. 2008.

[5] D. Barbara and T. Imielinski. Sleepers and workaholics: caching strategies in mobile environments (extended version). *The VLDB Journal*, 4:567–602, 1995.

[6] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. *USENIX Security Symposium*, 12:2–2, 2003.

[7] A. Boukercha, L. Xua, and K. EL-Khatibb. Trust-based security for wireless ad hoc and sensor networks. *Elsevier Computer Communications*, 30(11-12):2413–2427, September 2007.

[8] C.-Y. Wang C.-C. Hoh and R.-H. Hwang. Anycast routing protocol using swarm intelligence for ad hoc pervasive network. July 2006.

[9] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc networks. *IEEE Trans. on Mobile Computing*, 2(1):52–64, 2003.

[10] D. Chen, J. Deng, and P. K. Varshney. Protecting wireless networks against a denial of service attack based on virtual jamming. In *ACM MobiCom '03 Poster Session*, San Diego, CA, USA, September 14-19 2003.

[11] Z. Cheng and WB. Heinzelman. Flooding strategy for target discovery in wireless networks. *Wireless Networks*, 11:607–618, September 2005.

[12] A. Garcia and F. A. Pedraza. Rational swarm routing protocol for mobile ad-hoc wireless networks. ACM, July 2008.

[13] M. Gunes, U. Sorges, and I. Bouazizi. Ara-the ant-colony based routing algorithm for manets. 2002.

[14] J. Hall. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *In Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT)*, pages 201–206. Kranakis, 2004.

[15] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva. Directed diffusion for wireless sensor networking. *IEEE/ACM Trans. on Networking*, 11(1):2–16, February 2003.

[16] P. B. Jeon and G. Kesidis. Pheromone-aided robust multipath and multipriority routing in wireless manets. ACM, October 2005.

[17] T. Jiang and JS. Baras. Ant-based adaptive trust evidence distribution in manet. March 2004.

[18] Shudong Jin and Limin Wang. Content and service replication strategies in multi-hop wireless mesh networks. In *MSWiM '05: Proceedings of the 8th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 79–86, New York, NY, USA, 2005. ACM.

[19] Y.-J. Joung and S.-H. Huang. Tug-of-war: An adaptive and cost-optimal data storage and query mechanism in wireless sensor networks. In *Proc. of the 4th IEEE international conference on Distributed Computing in Sensor Systems (DCOSS âĂŹ08)*, pages 237–251, Berlin, Heidelberg, 2008. Springer-Verlag.

[20] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad hoc Networks*, 1, 2003.

[21] J. Kennedy. *Handbook of Nature-Inspired and Innovative Computing*. Springer US, 2006.

[22] Y. Kong, J. Deng, and S. R. Tate. A distributed public key caching scheme in large wireless networks. In *Proc. of IEEE Global Telecommunications Conference - Communication and Information System Security (GLOBECOM '10)*, Miami, FL, USA, December 6-10 2010.

[23] L. Lazos, R. Poovendran, and J.A. Ritcey. Analytic evaluation of target detection in heterogeneous wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, March 2009.

[24] M. Li and Y. Liu. Rendered path: Range-free localization in anisotropic sensor networks with holes. *Networking, IEEE/ACM Transactions on*, pages 320 – 332, Feb. 2010.

[25] X. Li, S. Gordon, and J. Slay. On demand public key management for wireless ad hoc networks. In *Proc. of Australian Telecommunication Networks and Applications Conference (ATNAC'04)*, pages 36–43, 2004.

[26] C. Lindemann and OP. Waldhorst. A distributed search service for peer-to-peer file sharing in mobile applications. page 73, September 2002.

[27] J. LÃşpez and J. Zhou. *Wireless Sensor Network Security.* IOS press, 2008.

[28] H. Miranda, S. Leggio, L. Rodrigues, and K. E. E. Raatikainen. An algorithm for dissemination and retrieval of information in wireless ad-hoc networks. In *Proc. of the 13th International Euro-Par Conference*, pages 891–900, France, 2007.

[29] S. Ni, Y. Tseng, and J. Sheu. The broaecast storm problem in a mobile ad hoc network. In *Proc. of the 5th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom '99)*, pages 152–162, Seattle, WA, USA, August 1999.

[30] P. Nuggehalli, V. Srinivasan, and CF. Chiasserini. Energy-efficient caching strategies in ad hoc wireless networks. In *Proc. of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 25–34, 2003.

[31] A. Proano and L. Lazos. Selective jamming attacks in wireless networks. *Communications (ICC), 2010 IEEE International Conference on*, May 2010.

[32] S. Radosavac, J.S. Baras, and I. Koutsopoulos. A framework for MAC protocol misbehavior detection in wireless networks. *Workshop on Wireless Security*, pages 33–42, 2005.

[33] S. Radosavac, A.A. CÃąrdenas, John S. Baras, and George V. Moustakides. Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers. *Journal of Computer Security*, 15:103–128, 2007.

[34] F. D. Rango and M. Tropea. Swarm intelligence based energy saving and load balancing in wireless ad hoc networks. ACM, June 2009.

[35] S. Ray, J.B. Carruthers, and D. Starobinski. RTS/CTS-induced congestion in ad hoc wireless lans. *Ad Hoc Wireless LANs*, 2003.

[36] M. Raya, J.-P. Hubaux, and I. Aad. DOMINO: a system to detect greedy behavior in ieee 802.11 hotspots. *International Conference On Mobile Systems, Applications And Services*, pages 84–97, 2004.

[37] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim. Highly reliable trust establishment scheme in ad hoc networks. *Computer Networks*, 45(6):687–699, August 2004.

[38] C. W. Reynolds. Flocks, herds and schools: A distributed behavioral model. ACM, 1987.

[39] Andrea Richa, Christian Scheideler, Stefan Schmid, and Jin Zhang. A jamming-resistant mac protocol for multi-hop wireless networks. In Nancy Lynch and Alexander Shvartsman, editors, *Distributed Computing*, volume 6343 of *Lecture Notes in Computer Science*, pages 179–193. Springer Berlin / Heidelberg, 2010.

[40] C.-C Shen, Z. Huang, and C. Jaikaeo. Ant-based distributed topology control algorithms for mobile ad hoc networks. *Mobile Networks and Applications*, 11, May 2005.

[41] C.-C Shen and C. Jaikaeo. Ad hoc multicast routing algorithm with swarm intelligence. *Mobile Networks and Applications*, 10, Feb. 2005.

[42] M. Strasser, B. Danev, and S. Capkun. Detection of reactive jamming in sensor networks. *ACM TOSN*, 2010.

[43] D. Subramanian, P. Druschel, and J Chen. Ants and reinforcement learning: A case study in routing in dynamic networks. In *Proc. International Joint Conference on Artifitial Intelligence*, pages 832–838, 1997.

[44] Y.-M. Tseng. A heterogeneous-network aided public-key management scheme for mobile ad hoc networks. *International Journal of Network Management*, 17(1):3–15, 2007.

[45] Johann Van Der Merwe, Dawoud Dawoud, and Stephen McDonald. Key distribution in mobile ad hoc networks based on message relaying. In *ESAS'07: Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks*, pages 87–100, Berlin, Heidelberg, 2007. Springer-Verlag.

[46] H. F. Wedde, M. Farooq, T. Pannenbaecker, B. Vogel, C. Mueller, J. Meth, and R. Jeruschkat. Beeadhoc: an energy efficient routing algorithm for mobile ad hoc networks inspired by bee behavior. ACM, 2005.

[47] H. F. Wedde, M. Farooq, and Y. Zhang. Beehive: An efficient fault-tolerant routing algorithm inspired by honey bee behavior. In M. Dorigo, M. Birattari, C. Blum, L. M. Gambardella, F. Mondada, and T. StÃijtzle, editors, *Ant Colony, Optimization and Swarm Intelligence*, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2004.

[48] Jianliang Xu, Qinglong Hu, Wang-Chien Lee, and Dik Lun Lee. Performance evaluation of an optimal cache replacement policy for wireless data dissemination. *IEEE Transactions on Knowledge and Data Engineering*, 16:125–139, 2004.

[49] W. Xu, W. Trappe, Y. Zhang, and T Wood. The feasibility of launching and detecting jamming attacks in wireless networks. *International Symposium on Mobile Ad Hoc Networking and Computing*, pages 46–57, 2005.

[50] Y. Xuan, Y. Shen, I. Shin, and T. M.T. On trigger detection against reactive jamming attacks: A clique-independent set based approach. *Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International*, Dec. 2009.

[51] J. Yick, B. Mukherjee, and D. Ghosal. Wireless sensor network survey. *Computer Networks*, 52, 2008.

[52] Wensheng Zhang, Guohong Cao, and Tom La Porta. Data dissemination with ring-based index for wireless sensor networks. *IEEE Transactions on Mobile Computing*, 6:832–847, 2007.

[53] Z. Zhang, J. Wu, J. Deng, and M. Qiu. Jamming ACK attack to wireless networks and a mitigation approach. In *Proc. of IEEE Global Telecommunications Conference / Wireless Networking Symposium (GLOBECOM '08)*, volume ECP.950, pages 1–5, New Orleans, LA, USA, November 30 - December 4 2008.

[54] L. Zhou and Z.J. Haas. Securing ad hoc networks. *IEEE Wireless Networks*, 13:24–30, August 2002.