Immunizing mobile ad hoc networks against collaborative attacks using cooperative immune model

Tao Gong[1,2,*,†], Bharat Bhargava[2]

[1] *College of Information Science and Technology, Donghua University, Shanghai 201620, China*

2 *Department of Computer Science, Purdue University, West Lafayette, IN 47907, U.S.A.*

CERIAS, Purdue University, 656 Oval Drive, West Lafayette, IN 47907-2086, U.S.A.

Summary

In this paper, a security problem of cooperative immunization against collaborative attacks such as blackhole attacks and wormhole attacks, in the mobile ad hoc networks such as the Worldwide Interoperability for Microwave Access (WiMAX) networks, was discussed. Due to the vulnerabilities of the protocol suites, collaborative attacks in the mobile ad hoc networks can cause more damages than individual attacks. In human immune system, non-selfs (i.e. viruses, bacteria and cancers etc.) can attack human body in a collaborative way, and cause diseases in the human body. Inspiring from the human immune system, a tri-tier cooperative immune model was built to detect and eliminate the collaborative attacks (i.e. non-selfs) in the mobile ad hoc networks. ARM-based Network Simulator (NS2) tests and probability analysis were utilized in the prototype for immune model to analyze and detect the attacks. Experimental results demonstrate the validation and effectiveness of the model proposed, by minimizing the collaborative attacks and immunizing the mobile ad hoc networks.

KEY WORDS: Cooperative immune model; ad hoc networks; security; collaborative attacks

1. Introduction

Security is a key challenge in the networks of Worldwide Interoperability for Microwave Access (WiMAX), which provides a high-speed broadband access (up to 40 Mbps) with large coverage in the IEEE 802.16 standard and so is more flexible and usable in many scenarios than the other technologies such as DSL or WiFi. But the shelf protocols of these networks make the vulnerabilities of those protocols available to attackers. For example, the availability of practical swarm intelligence and multi-agent algorithms can help attackers to collaborate and realize more effective attacks against defending mechanisms [1, 2]. The current WiMAX systems use some individualized security approaches such as antivirus software [3], intrusion detection tools [4], and mail filtering applications [5] etc. However, the WiMAX network is not secure against collaborative attacks because the security approaches are suitable for only individual attacks. Collaborative attacks are launched by some malicious adversaries to accomplish disruption, deception, usurpation or disclosure against the targeted networks [1].

*Correspondence to: Tao Gong, Department of Computer Sciences, Purdue University, West Lafayette, IN, USA.

†E-mail: tgong@purdue.edu

For instance, if the SYN flood attack and the slammer worm are launched in a coordinated way, the resulting consequences will be devastating and very difficult to deal with [6, 7]. What's more, many attackers can influence the decision-making of some core machines with Sybil attacks in WiMAX [8].

To deal with the collaborative attacks, some cooperative approaches are designed and used for matching the features of multiple attacks in collaborative ways. Unfortunately these approaches are often ineffective to unknown attacks [3]. In fact, human immune network is an advanced natural cooperative defending system against collaborative attacks from viruses, bacteria and cancer [9]. Both RNA-containing and DNA-containing viruses, two obviously different classes of virus, can cause cancer [10], and so bacteria with the viruses and cancer can cause the overload and damages of the immune system. Thus, the biological immune network inspires us to design more advanced defense system against the collaborative attacks. In general, the human immune network has a large number of immune cells (e.g. B cells and T cells) and immune molecules (e.g. antibodies). In many cooperative immune responses, the immune cells and immune molecules make up the parallel immune tier, which realize immune responses in parallel cells and molecules [11]. At first, the immune network against the attacks determines whether the strange objects are selfs and detect the attacks [12]. If they are selfs, the objects are not relative with the attacks; otherwise, the objects are the non-selfs that cause the attacks. Detecting the selfs and the attacks is the first mission of the native immune tier, and recognizing and classifying the known attacks are the other responsibilities of the tier. To recognize the unknown attacks, immune learning and memory are required for the adaptive immune tier of immune network [13].

According to the bio-inspired ideas, an anti-worm static artificial immune system was proposed and evaluated based on the tri-tier immune model [14]. The immune model was also used in software fault diagnosis of mobile robots [15]. In this paper, a novel cooperative immune model against the collaborative attacks such as blackhole attacks and wormhole attacks in the mobile ad hoc networks was proposed and evaluated to detect the attacks and minimize the attacks. In section 2, the related work was analyzed on security, the collaborative attacks and artificial immune systems (AIS) for this security application. The cooperative immune model was proposed against the collaborative attacks in the mobile ad hoc networks in section 3. In section 4, the detection and learning capabilities of the immune model in a cooperative way was analyzed. In section 5, the experiments of the cooperative immune network against the collaborative attacks were realized in the NS2 networks with the ARM nodes. Section 6 concluded the paper.

2. Related work

The vulnerabilities of the mobile ad hoc networks have been analyzed in the literature. In the following the main characteristics of the vulnerabilities were reviewed briefly.

Bhargava et al. regarded the support to DES as an important vulnerability in WiMAX standards, because DES can be broken by the collaborative attacks [1]. Second, attacks through the IEEE 802.16j standard include blackhole attacks [16], wormhole attacks [17], denial-of- message attacks [18] and Sybil attacks [19] etc. Besides, the implementation bugs and the incompatibilities are also the potential sources of vulnerabilities [1].

For instance, blackhole attack can transmit malicious broadcast information from a node that the node has the shortest path to the destination aiming to intercept messages [16]. Wormhole attack can record packets at one

location in the network, tunnel them to other locations, and retransmit them there into the network [17, 20]. The collaborative attacks of blackhole and wormhole almost have all the abilities of the two attacks [2].

To defend against the collaborative attacks, a few of cooperative approaches have been proposed recently. For example, Cheung et al. decomposed some cyber attacks into multiple sub- attacks and developed a method to model multistep attack scenarios based on typical isolated alerts about attack steps [21]. Li et al. built a stochastic model of collaborative internal and external attacks [22]. Yang et al. designed a signature-based model to detect collaborative attacks [23]. Based on multicast, annotated topology information, and blind detection techniques, Hussain et al. built a collaborative system to detect distributed DoS (DDoS) attacks [24]. Ourston et al. used Hidden Markov models to detect collaborative attacks [25]. Cuppens et al. made each Intrusion Detection System (IDS) in some collaborative IDSs send its triggered alerts to a central module, in order to reduce the number of false positives [26]. The central module correlates the incoming alerts of all IDSs and generated a more elaborated and general alarm to the whole system. Lin et al. shared the information from the node that detected the intrusion to the other nodes, so that they can save time and energy for doing pattern matching which is a demanding task [27]. Yu-Sung et al. proposed a collaborative intrusion detection system for different sorts of IDSs to work cooperatively [28].

To overcome the disadvantages of the IDS approaches against the unknown attacks, the techniques of immune computation have been investigated for some security applications, especially in the mobile ad hoc networks. Sarafijanovic et al. used an artificial immune system to detect node misbehavior in a mobile ad hoc network using the dynamic source routing (DSR) protocol [29]. Mohamed et al. presented the immune-inspired security architecture for simulating a number of human immune system (HIS) processes for securing mobile ad hoc networks [30]. Atakan et al. introduced an immune-system-inspired evolutionary opportunistic spectrum access (ESA) protocol, based on the self-nonself detection and clonal selection principles [31].

As one of the security foundations, threat modeling is defined as a systematic exploration technique to expose any circumstance or event having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service, and results in a vulnerability assessment [32]. Thus, threat modeling or other exploratory techniques shall be applied to explore known and potential security vulnerabilities and their impacts. Bau et al. illustrated security analysis using model checking, but analysts can use various methods and tools to evaluate system security, including manual and automated theorem-proving tools that provide assurance about the absence of attacks in a specified threat model [33]. Similar to the threat model, the immune danger theory was proposed by Matzinger [34], and in this danger theory immune response distinguishes the danger signals that are generated by damaged cells. In the AIS, the threats are the damaged selfs and the foreign non-selfs, so the threats are the non-selfs in nature. The vulnerabilities of the AIS depend on its design in security.

3. Cooperative immunization model against collaborative attacks

The collaborative attacks here are defined as two or more types of attacks such as the blackhole attacks and the wormhole attacks, which can attack the mobile ad hoc network in a collaborative way.

Suppose a mobile ad hoc network such as the WiMAX network is represented as finite immune graph $G=(V, E)$, where V is the vertex

or node set, and E is the edge set with $E \neq \phi$. An element in the set V represents a client, server or cloud in the mobile ad hoc network, and any element in the set E represents the relationship between one client/server and another one. It is assumed that the edges are undirected and the graph is connected. When the system initializes, the mobile ad hoc network without any attacks is normal, which is identified by the space-time representation of its normal model [9]. It is also assumed that a unique discrete time order is represented with t=0, 1, 2…, though the time properties of some components may be turned back or changed forward with a big step in a local virtual space. Considering the attacks such as the blackhole attacks and the wormhole attacks in a sequential order, a node is secure, damaged, or removed at any point in time. Suppose the blackhole attacks are represented with $A^1 = \{a_i^1 \mid i = 1,2,\ldots,N^1\}$, and N^1 represents the sum of the blackhole-attack nodes. And $A^2 = \{a_j^2 \mid j = 1,2,\ldots,N^2\}$ denotes the wormhole attacks, and N^2 represents the sum of the blackhole-attack nodes. Thus, the problem on defending against the collaborative attacks such as the blackhole attacks and the wormhole attacks is how the two types of attacks can be detected and eliminated. For calculating the sum of the attacks, this problem on defending against the attacks is formulated below.

$$\text{Min} \sum_{k=1}^{2} N^k . \quad (1)$$

Because the attack detection is the first important step for minimizing the damages that are caused by the attacks, this problem has an important sub-problem of maximizing the attack-detection probability below.

$$\text{Max} \frac{1}{2} \sum_{k=1}^{2} p^k , \quad (2)$$

where p^1 denotes the success probability for detecting the blackhole attacks, and p^1 denotes the success probability for detecting the wormhole attacks. Moreover, at the same time the performances, such as the packet delivery ratio (PDR), throughput, overhead and end-to-end delay, should be optimized by the network reconfiguration of immunization.

Based on the tri-tier immune model, which is of the native immune tier, the adaptive immune tier and the parallel immune tier, as shown in Figure 1, new tri-tier architecture for securing the mobile ad hoc networks such as WiMAX networks was proposed as shown in Figure 2 [35]. As the first tier, the native immune tier is used to detect attacks in a cooperative way, and the self is the most important factor in increasing the efficiency and effectiveness of the attack detection process. Besides, the native immune tier is also responsible for recognizing the known attacks. The second tier is adaptive immune tier that is used to learn and recognize unknown attacks cooperatively, based on the expendable multi-dimension feature space of attacks. To minimize the collaborative attacks, the cooperative immunization works with the inputs of all objects in the mobile ad hoc networks in the following way.

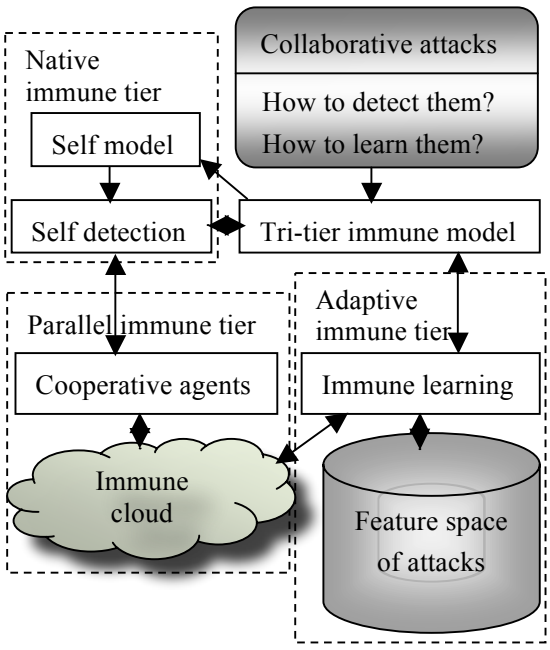

Fig. 1. Tri-tier cooperative immune model.

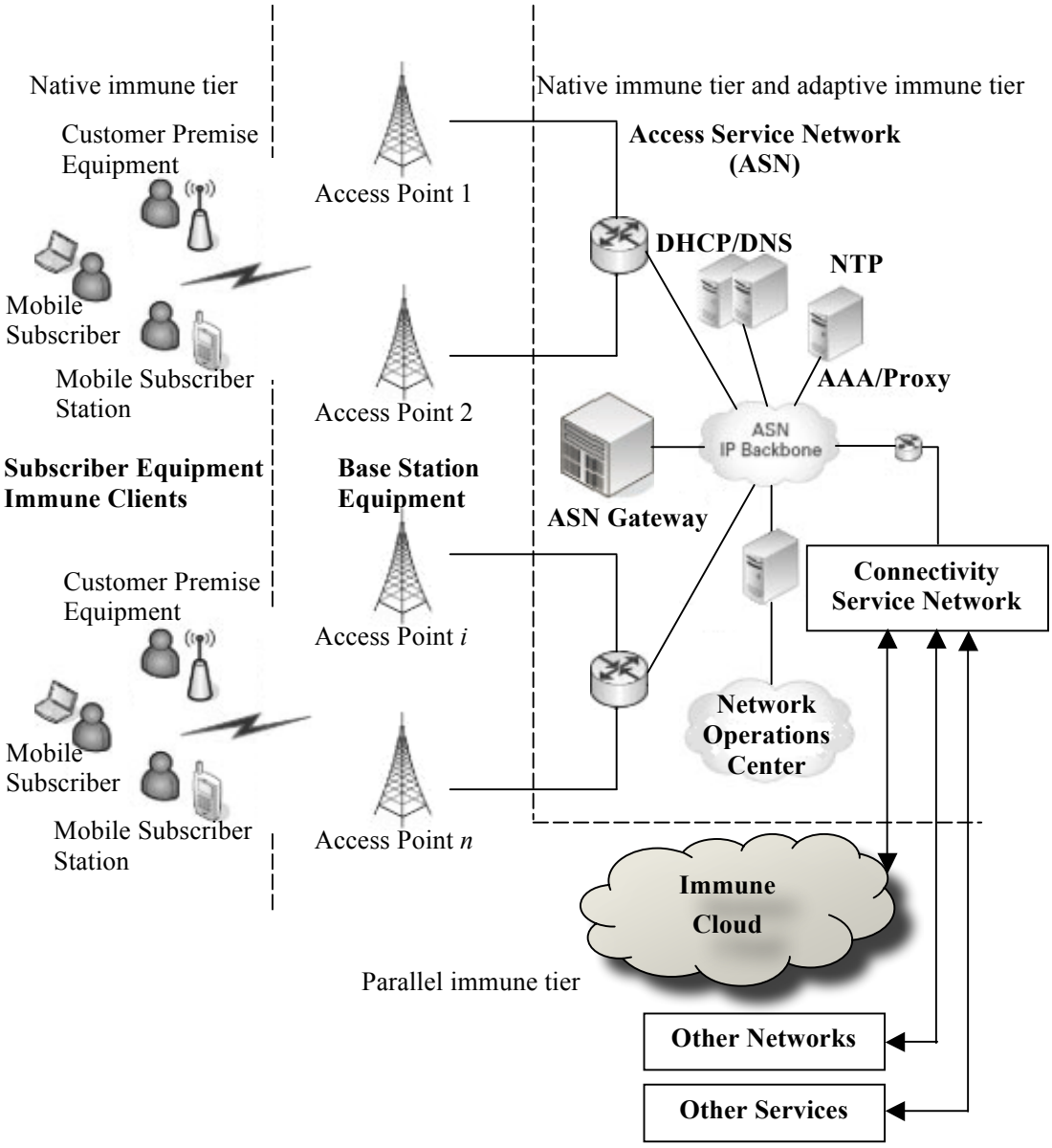

Fig. 2. WiMAX immunization architecture.

First, the native immune tier detects the selfs, which are defined here as the normal components of the mobile ad hoc network. The self model is of the space-time properties for the normal states to increase the precision of self detection, as shown in Figure 1. When the mobile ad hoc network is normal, the space-time properties, which identify the self status, of the normal components are stored into the self database. The tri-tier immune model is based on the self model and the self detection, because the results for detecting the selfs in the first step of immunization can be used to detect more attacks more quickly than the approach for detecting the attacks directly. For example, the wormhole attacks attempt to modify the routing protocol files and the routing table files of the attacked node, so that the wormhole attacks can transmit their own attacking codes to other nodes from the compromised node by sending some attacking packets. Before the wormhole attacks occur, all the normal nodes of the mobile ad hoc network such as the WiMAX network store their space-time properties of each files in the nodes into a secure self database, and the

space-time properties of the files can be the absolute pathnames and the last revision time. Once any file of the core parts in any node is modified by the wormhole attacks to change the protocol and the routing table, the self detection through the self database will return an alert of detected non-self, i.e. the wormhole attacks. Because the selfs of the normal components are well known for the system, it is easier to detect whether a node is a self than to detect whether the node is a compromised one by unknown attacks by recognizing the unknown features of the attacks. Moreover, when the self model is damaged unfortunately the immune learning of the adaptive immune tier and the immune cloud of the parallel immune tier can be used to detect the attacks by matching the features of the non-selfs, as shown in Figure 1. Though the compromised node, whose self model may be damaged by the attacks, cannot detect the damages with its self model, the other nodes that are attacked by this node will detect the attacks with the normal model and the features of the damaged files in the compromised node.

For instance, when an attack is detected, the source node of the attack may be a normal one in the past and now damaged by the attack. This determination depends on whether the space property of the source node is already in the self database. If the search of this space property in the self database returns nothing, the source node of the attack is sure a new attacking node. The non-selfs are defined here as both the damaged components and the new attacking nodes, which are not acceptable for the immune mobile ad hoc network. The non-selfs are eliminated and the damaged components are repaired finally.

In the third tier, the immune cloud is a new parallel computing system, which is built with the cloud computing infrastructure. The cloud- based parallel immune tier is used to increase both the efficiency and robustness of immune computation. In Figure 1, the immune learning is made by searching the most similar known attacks in the feature space of attacks. In Figure 2, the subscriber client, the access service network and the connectivity service network in the WiMAX have different self models, and they can work cooperatively when any attack is detected. Because the subscriber client, the access service network and the connectivity service network all have the normal-model-based immune mechanisms that are similar to immune cells, they can detect the attacks and eliminate the attacks in a similar way that the biological immune cells defend against the viruses cooperatively. For example, when a subscriber client detects an attack with its immune mechanism and report both the position and features of the attack to the immune interfaces of the access service network and the connectivity service network, the two service network will activate their immune programs to detect the attack from the found position through the mobile ad hoc network. At the same time, the connectivity network may inform some external networks to detect the attack if the attack comes from any node of any external network or already goes out to any node of any external network.

After an attack is detected at any part of the network, the information about the attack will be sent to the relative clients and networks to activate the immune responses against the attack in the relative clients and networks. Afterwards, the attacks that have been detected will be recognized by matching their available features in the expendable feature space of all the known attacks with the real-time searching algorithms, and the pattern recognition will be made in a cooperative way via the servers and cloud computing platform. The servers can be installed in both the access service network and the connectivity service network. If the search result is yes, then the attacks will be controlled and cleared in a

relatively easy way, and both the features and the research result of the attacks will be delivered to the relative clients and networks to eliminate the attacks and defend the system. If the search result is no, then the attacks will be learnt with some intelligent methods such as enhanced learning from examples and learning based on neural network etc., and the immune learning is partly built on the cloud computing and cooperation of the servers in both the access service network and the connectivity service network.

4. Analysis of immune model

When a node in the mobile ad hoc network, defined in section 3, is damaged by the attacks, it may be under control of attackers, and thus may attack other nodes as a tool of the attackers. The attacks may remove crucial nodes, and the damaged nodes may be removed in its immune response in order to be repaired by its backup ones. So it is assumed that the mobile ad hoc network such as WiMAX network has m clients, n servers (called AServer) in the Access Service Network, l servers (called as CServer) in the Connectivity Service Network, and d immune clouds. The immune clouds are built on cloud computing to increase the speed and efficiency of the artificial immune system.

First of all, the set of nodes, which were damaged by the attacks at or before time t, is denoted by D_t. $N(t)$ is used to denote the number of nodes that were damaged at or before time t, and the number of nodes, which were removed or lost by time t, was denoted by $M(t)$. Therefore, $N(t)$-$M(t)$ is used to denote the number of nodes that were damaged but have not been removed by time t. For the event that the node was damaged, the degree of node v ($v \in V$) in G is denoted by deg(v), and the set of nodes neighboring with the node v is denoted by $\{v' \mid (v, v') \in E\}$. The time, at which the kth node changes state from secure to damaged (i.e. the kth incident occurs), is denoted by T_k, where $1 \le k \le |V|$. And the identity of the node, which was damaged by the attacks at time T_k, i.e. the kth damaged node, is denoted by node(T_k). Suppose for any sequence of damaged nodes node(T_1), …, node(T_i), …, node($T_{|V|}$), the degree of node(T_i) follows distribution D_i ($1 \le i \le |V|$), which is distributed identically and independently as the degree distribution D of G=(V, E) [22].

For random variables R_1 & R_2, if $\Pr[R_1>k] \ge \Pr[R_2>k]$ for any k, then R_1 is called larger (or faster) stochastically than R_2, denoted by $R_1 \succeq_{st} R_2$ [36]. Thus, for the sequence of the stochastic intervals between two incidents (e.g. the ith incident and the succeeding incident) occurrences, which are denoted by $S_{1i}=T_{i+1}-T_i$ for i=0, 1, …, $|V|$-1, the sequence S_0, S_1, …, S_k is stochastically decreasing that is denoted by the following formula [22]:

$$S_i \succeq_{st} S_{i+1}, i = 0,1,\cdots,|V|-1. \quad (3)$$

This proposition is used to prove that the coordinated attacks become more powerful as more internal nodes are damaged and produce new attacks. Here, the discretization makes T_k follows a discrete Poisson process of success probabilities r_{k-1} for k= 1, …, $|V|$ [22], and the probabilities r_{k-1} are denoted by the following formula:

$$r_i = \frac{|V| + d_1 + d_2 + \cdots + d_i - i}{2|E| + |V|}, \quad r_0 \underset{def}{=} \frac{|V|}{2|E| + |V|}, i = 1,2,\cdots,|V|-1 \quad (4)$$

Here, $d_j = \deg(\text{node}(T_j))$ for j=1, $|V|$.

After the damaged node node(T_i) is detected, the node should be isolated immediately by cutting off the damaged node's output. It is assumed that the success probability of detecting the damaged node is denoted by p_i and so the success probability of cutting off

the output of the damaged node equals to p_i. Therefore, according to (4), the probability r_i with detection is improved by the following formula:

$$r_i = \frac{|V| + \sum_{j=1}^{i-1} d_j + d_i \cdot (1 - p_i) - i + 1 - p_i}{2|E| + |V|} = \frac{|V| + \sum_{j=1}^{i} d_j - p_i \cdot (d_i + 1) - i + 1}{2|E| + |V|}, \quad (5)$$

In general, there are 3 strategies to find the damaged node: (1) attack detection directly by getting and matching the features of the damaged node in the feature space F_B for the incomplete set B of attacks, with measuring errors; (2) unknown attack learning from the feature space F_A for the complete set A of all known attacks, with uncertain results of detection and recognition; (3) self detection based on the space-time property set F_S of the selfs and the normal model for defining the selfs, and then non-self detection based on the results of the self detection. For strategy 1 and strategy 2, if the node is damaged by the known attacks, then the success probability $p_i^{(1)}$ for strategy 1 can be denoted by the following formula:

$$p_i^{(1)} = \frac{|F_B|}{|F_A|} \cdot p_e^{(1)}, i = 1, \cdots, |V|, \quad (6)$$

Here, the probability of measuring errors for strategy 1 is denoted by $p_e^{(1)}$, and the success probability $p_i^{(2)}$ for strategy 2 is denoted by the following formula:

$$p_i^{(2)} = p_l \cdot p_e^{(2)}, i = 1, \cdots, |V|, \quad (7)$$

Here, the probability of measuring errors for strategy 2 is denoted by $p_e^{(2)}$, and the success probability of learning unknown attacks is denoted by p_l. Thus, $p_e^{(2)} \approx p_e^{(1)}$, $p_l = 1$.

Thus, the following theorem is correct:

$$p_i^{(1)} \le p_i^{(2)}, \quad (8)$$

$$r_i^{(1)} \ge r_i^{(2)}. \quad (9)$$

Here, for $\gamma \in \{1,2,3\}$, the sequence of geometric success probabilities for detection strategy γ is denoted by $r_1^{(\gamma)}, \cdots, r_k^{(\gamma)}$.

If the node is damaged by unknown attacks, then the success probability $p_i^{(1)}$ for strategy 1 always equals to 0 because the features of the unknown attacks will not be matched in the feature space F_B; to our hope the success probability $p_i^{(2)}$ depends on learning [37, 38, 39, 40, 41], and the following experience formula is mostly correct:

$$0 = \frac{|F_B|}{|F_A|} < p_l \le 0.8. \quad (10)$$

Thus, (8) and (9) are still correct.

When the space-time property set F_S is normal with the correct data for strategy 3, no matter whether the node is damaged by the known attacks or not, the success probability $p_i^{(3)}$ for strategy 3 can be denoted by the following formula:

$$p_i^{(3)} = p_s \cdot p_e^{(3)}, i = 1, \cdots, |V|, \quad (11)$$

Here, the probability of measuring errors for strategy 3 is denoted by $p_e^{(3)}$, and the success probability of detecting the selfs is denoted by p_s. Moreover, $p_e^{(3)} \approx p_e^{(2)} \approx p_e^{(1)}$, $p_s = 1$.

Thus, when the node is damaged by known attacks,

$$p_i^{(3)} \approx p_i^{(2)} \ge p_i^{(1)}, \quad (12)$$

$$r_i^{(3)} \approx r_i^{(2)} \le r_i^{(1)}. \quad (13)$$

But, when the node is damaged by some unknown attacks, according to (10),

$$1 = p_S > 0.8 \ge p_l > \frac{|F_B|}{|F_A|} = 0. \quad (14)$$

$$\therefore\ p_S \cdot p_\varepsilon^{(3)} > p_l \cdot p_\varepsilon^{(2)} > \frac{|F_B|}{|F_A|} \cdot p_\varepsilon^{(1)}. \quad (15)$$

$$\therefore p_i^{(3)} > p_i^{(2)} > p_i^{(1)}, \quad (16)$$

$$\therefore r_i^{(3)} < r_i^{(2)} < r_i^{(1)}. \quad (17)$$

In summary, for any attack,

$$r_i^{(3)} \le r_i^{(2)} \le r_i^{(1)}. \quad (18)$$

For $\gamma \in \{1,2,3\}$, the time at which the kth incident due to attacks occurs for detection strategy γ is denoted by $T_k^{(\gamma)}$ [22], then for k=1, 2, …, |V|, the theorem below is correct:

$$T_k^{(3)} \ge T_k^{(2)} \ge T_k^{(1)}. \quad (19)$$

This proposition is useful, for it inspires us, from the perspective for fighting against the attacks, that detection strategy 3 outperforms detection strategy2, which in turn outperforms detection strategy 1. In fact, because some of the collaborative attacks are known and the others are often unknown, if the space-time property set F_S is normal with correct data, strategy 3 is the best approach to test the attacks; otherwise, strategy 2 is often better than strategy 1, especially in dealing with the unknown attacks.

5. Simulation results and analysis

Network Simulator 2.35 and the ARM-based nodes were utilized to build the experiment platform [42]. Some nodes were designed with the ARM systems, and each ARM node communicated with other nodes in the network by Zigbee modules. The normal states of the ARM systems were identified with the unique normal model for selfs, and the normal model stored the space-time properties of the normal components, such as the absolute pathname and the last revision time of the normal files. Both the blackhole attacks and the wormhole attacks are implemented as two new attacking AODV-based protocols with C++ in the NS2-based Linux environment. When any attack tried to change the ARM system to expand the damages, the immune algorithms would detect the attacks by checking the space-time properties of the selfs according to the normal model of the selfs. Because the normal model was unique and protected well, the self detection was quick and effective, so that the results for detecting the selfs were used to increase the effectiveness and efficiency for detecting the attacks. Besides, the system repairing was also based on the normal model to keep high precision and efficiency, and the backup system of the normal ARM system was also used to repair the damaged components without affecting other normal components. The parameters for implementing and comparing the results of the experiments were shown in Table 1. The purpose of this experiment is to show that the immune mechanism based on the normal model can be deployed in small-scale mobile ad hoc networks to detect and repair the collaborative attacks such as blackhole attacks in collaboration with wormhole attacks.

Table 1. Parameter setting of experiments with NS2 and ARM nodes. CBR represents the constant bit rate.

Parameter name	Initial value
Simulation time	90(s)
Sum of mobile nodes	4, 16
Sum of static nodes	3
Sum of base-station node	1
Sum of blackhole nodes	3
Sum of wormhole node	1
Topology	700m*700m
Normal routing protocol	AODV
Blackhole attack protocol	blackholeAODV
Wormhole attack protocol	wormholeAODV
Traffic	CBR
Normal packet size	512bytes
Abnormal packet size	1024bytes
Data rates	10Kbits
Sum of ARM nodes	3
Sum of backup system	1

The topology for the proposed architecture was used into the simulation of collaborative attacks in the mobile ad hoc networks. This scenario consisted of 4 or 16 mobile nodes, 3 static nodes and 1 base-station node. The basic AODV routing protocol was used and UDP packets were sent and received among the nodes. Based on the AODV routing protocol, the blackhole attacks and the wormhole attacks were simulated with such protocols as blackholeAODV and wormholeAODV.

The velocity of the mobile nodes is changeable and the increasing velocity can speed up the spread of the attacks and also activate the immune detection against the attacks more quickly. For example, when the first mobile node changed its velocity from 10.651114437597 *m*/*s* to 30.297753834616 *m*/*s* and moved towards the other nodes, the other compromised nodes could attack the first mobile node sooner. When the second mobile node changed its velocity from 38.667612113725 *m*/*s* to 0.290700863224 *m*/*s* and moved towards the other nodes, this node would be later into the attacking range of the other compromised nodes. So the speedup of attacking activated earlier immune detection of the attacks, and the delay of the attacking time caused the immune detection delay of the attacks. However, once the attacking codes tried to change the core codes of the first mobile node or the second one, the immunization was always activated upon the detection of the attacking codes.

The immunization mechanism was used to cut off the connection between the attacked node and other normal nodes and make the attacked node repaired. All simulation runs lasted 90 seconds, and to avoid disturbances from the warm-up period, the first 8 second of the simulation results should be discarded.

Particularly, 2 normal network scenarios, 6 different attack scenarios and 4 different anti-attack scenarios were simulated. In the attack scenarios, the effect of single blackhole attack, the effect of single wormhole attack and the combined effect of blackhole attack together with wormhole attack on the performance of ad hoc wireless networks were analyzed. The anti-attack scenarios with different approaches were conducted and compared to evaluate the defending mechanism for keeping the network robust against collaborative attacks [2].

For these evaluations, the reaction time included the detection time and the response time. Different detection approaches spent different time, which might cause important difficulty to eliminate and defend the attacks. In order to improve the accuracy of the test, multiple repeated attacks were conducted to each experiment. In these experiments, 4 important metrics were evaluated, i.e. PDR, throughput, overhead and end-to-end delay. PDR is denoted with the ratio between the amount of packet delivered at the destination node and the whole amount of sent packets by the source node. Throughput and end-to-end delay are used to show the network performance degradation. Besides, overhead is represented with the fraction of all control packets sent during the simulation time out of the total amount of packets transmitted.

Figure 3 shows the PDR in four types of 8-node networks, and Figure 4 shows the PDR in four types of 20-node networks. 20 nodes are fit to show the characters of the mobile ad hoc network in the NS2, because too many nodes will cause overload in generating .nam files. The first network was normal one; the second was damaged by the blackhole attacks on three nodes; the third was damaged by the wormhole attack on another node and the last one was damaged by the collaborative attacks. The networks under the attacks had lower packet delivery ratios than the normal network, and the four curves in different positions and trends show that the collaborative attacks are more harmful than single attacks.

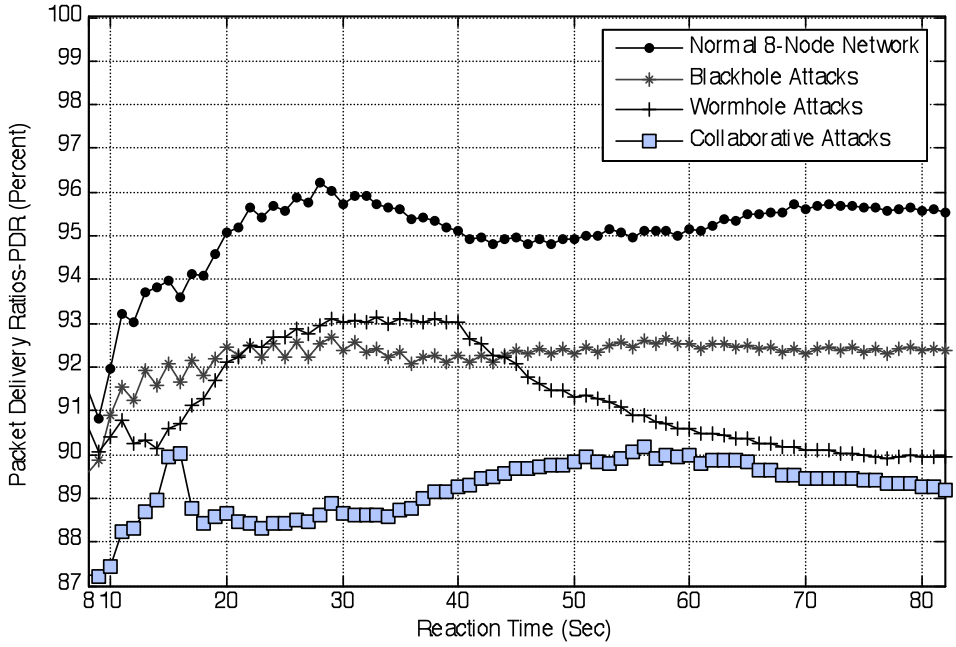

Fig. 3. Packet delivery ratios of the 8-node networks under attacks including collaborative attacks.

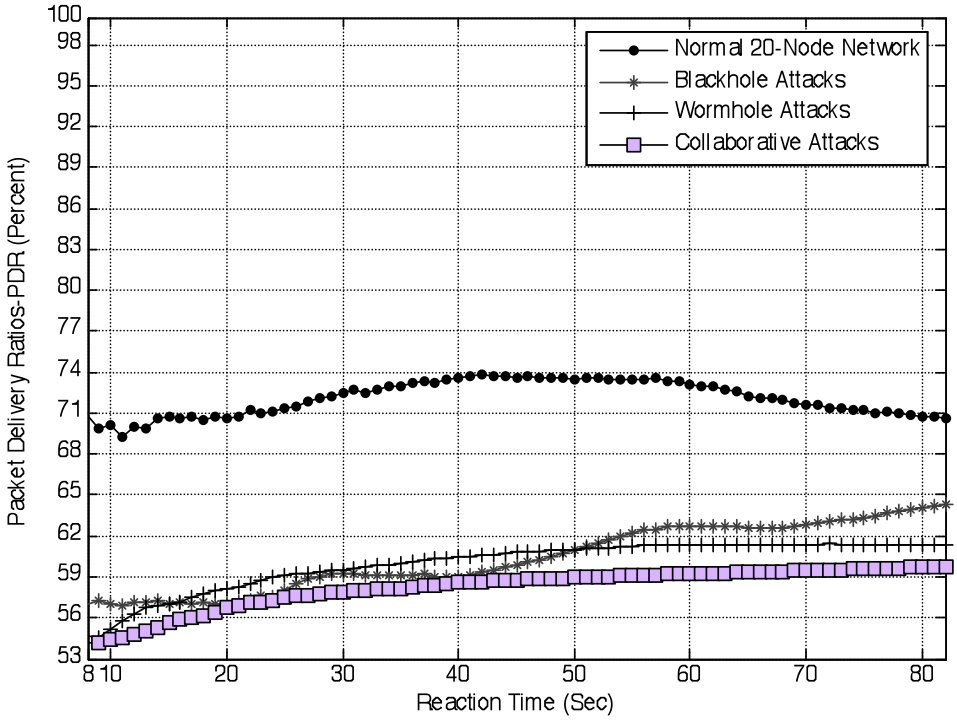

Fig. 4. Packet delivery ratios of the 20-node networks under the attacks.

Both the 8-node network with cooperative immunization and the 20-node network with cooperative immunization performed better than the network with IDS in Figure 5 and Figure 6 respectively. Once the network was immunized at 12 second in Figure 5, the packet delivery ratio of the 8-node network being immunized was sure higher than those of the network with regular IDS and the network under the collaborative attacks.

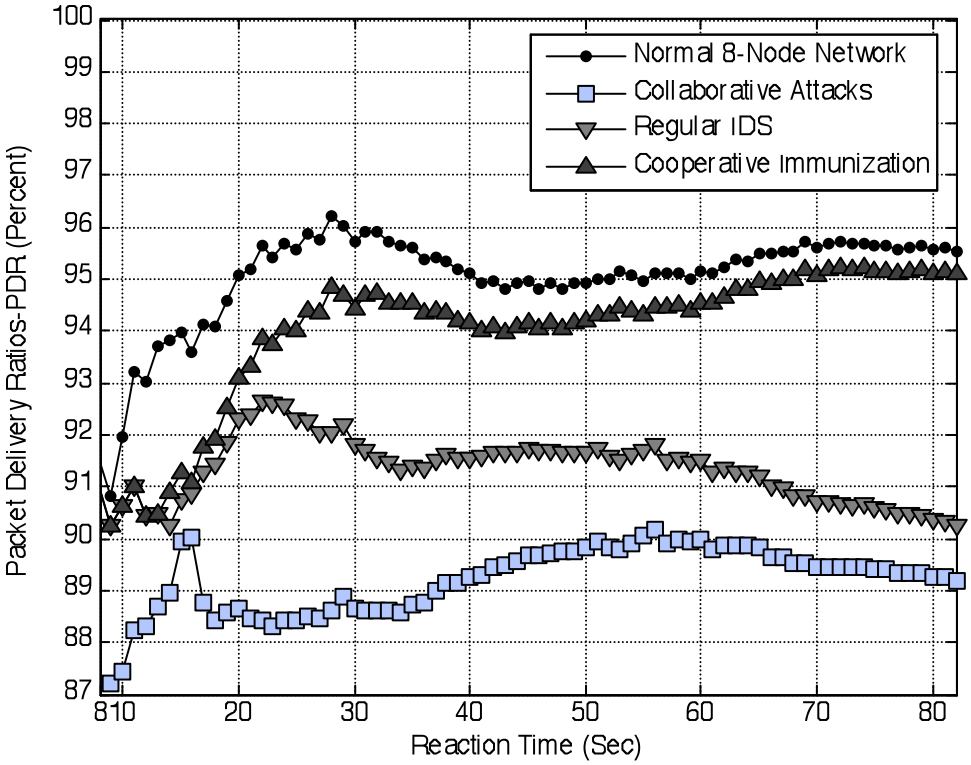

Fig. 5. Packet delivery ratios of the 8-node networks defending against collaborative attacks.

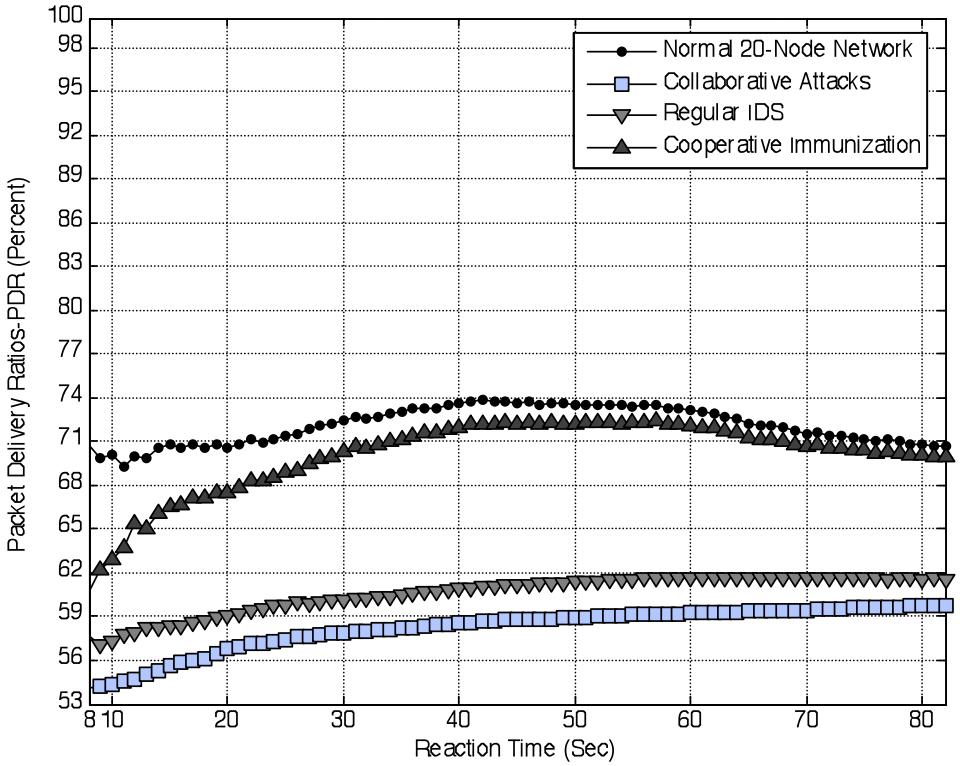

Fig. 6. Packet delivery ratios of the 20-node networks defending against collaborative attacks.

The regular IDS mechanism can detect the known attacks such as the blackhole attacks, but this approach cannot detect the unknown wormhole attacks with learning mechanism.

For comparing the performances of the two defense approaches, the throughputs of the connections in the different 8-node networks were measured and analyzed in Figure 7. It is sure to affirm that regular IDS caused higher throughputs due to the harmful expansion of wormhole nodes, but the node under wormhole attacks was isolated and the normal nodes were well protected by the immune network based on the normal model.

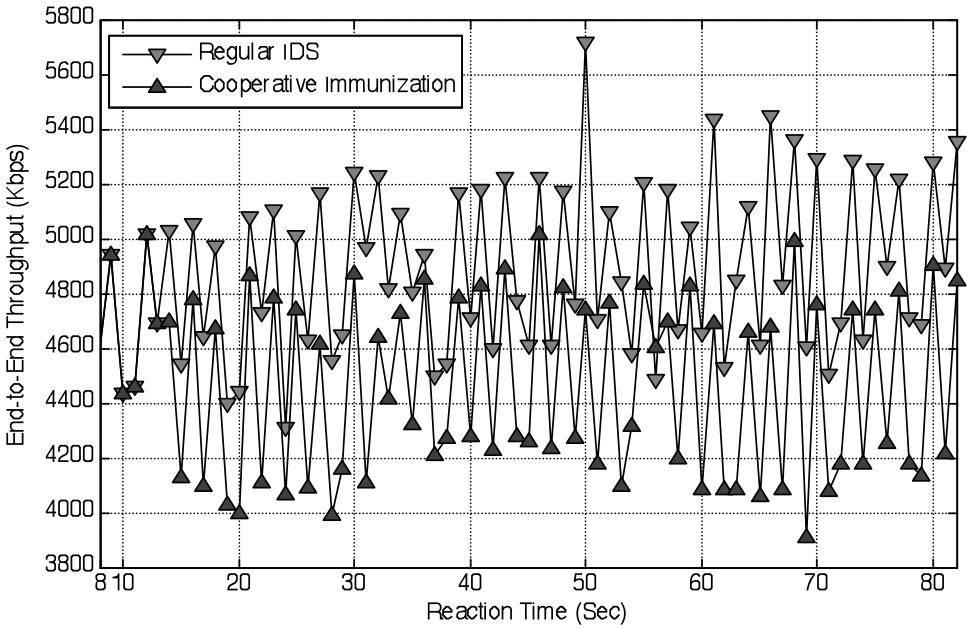

Fig. 7. End-to-end throughput.

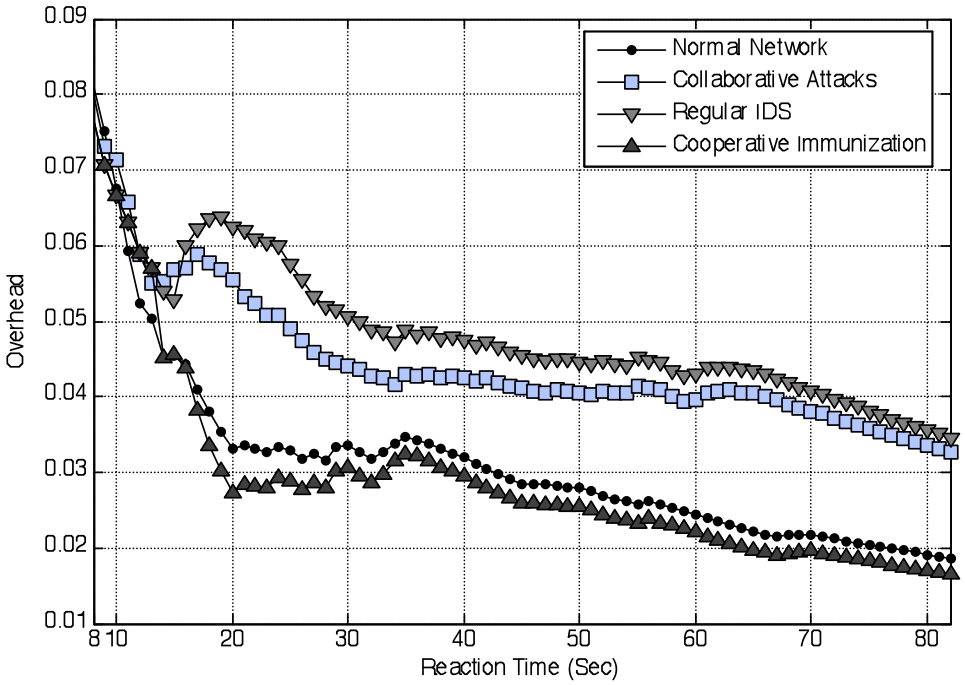

Fig. 8. Overall overhead.

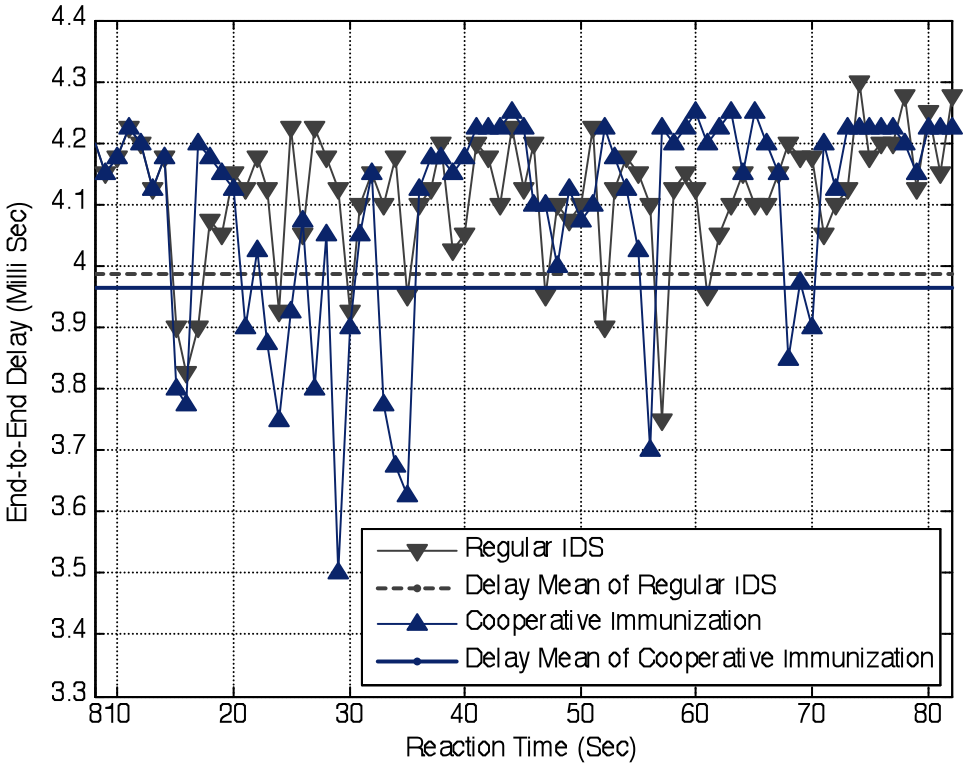

Fig. 9. End-to-end delay.

The next metric evaluated was the network overhead, which shows how much of control packets were generated within the 8-node network, as shown in Figure 8. Both the normal network and the immune network performed better than the network under collaborative attacks and the network with regular IDS against the attacks. The immune network first performed worst due to the attacks without beginning the immune responses. The higher the reaction time becomes, the better overall performance of the proposed immunization scheme will be.

The last observed metric, the end-to-end delay of the 8-node network, is shown and compared in Figure 9. The results in this figure were calculated by taking the average of the end-to-end delay of the incoming packets at the receiver. As same as the previous, the end-to-end delay stresses the more chance of better performance for the wireless network by immunization.

Overall, the experimental results on the NS2 and the ARM nodes allow affirming that it is important and useful for the wireless WiMAX network to utilize the cooperative immunization for security. Based on analyzing the experiment results, the immunization has three advantages than the regular IDS. First, the immunization is able to isolate the nodes under attacks by the network reconfiguration; second, the immunization can identify the nodes under attacks by detecting the non-selfs and the selfs based on the normal model, which is useful and crucial for controlling and eliminating the fast expansion of the active attacks such as the wormhole attacks; finally, the immunization is of new powerful learning mechanism for defending the networks, called as immune learning.

6. Conclusions and future works

Some important properties and mechanisms of cooperative immunization were proposed to

defend the ad hoc network under such collaborative attacks as the blackhole attacks and the wormhole attacks. New tri-tier cooperative immunization based framework was designed to detect and recognize the collaborative attacks in mobile ad hoc networks such as WiMAX networks. The performance of the proposed framework was analyzed in term of the packet delivery ratios, the throughput, the traffic overhead, and the responsiveness of the system. The experimental results confirm the effectiveness of the proposed cooperative immune model in detecting and mitigating these collaborative attacks from disrupting the protected mobile ad hoc networks such as WiMAX networks.

For future works, it is interesting to design the products of the proposed framework with the optimal parameters to keep the mobile ad hoc network secure. Another future research is to improve the protocols of immunization by increasing the accuracy and speed of the adaptive immunization in dealing with unknown attacks. Evaluations of the issues such as tests against other collaborative attacks, real-time identification of the selfs, complexity, optimization, and consumption are also left for future work.

Acknowledgements

The work was supported in part by grants from Natural Science Foundation of Shanghai (08ZR1400400), the Shanghai Educational Development Foundation (2007CG42), the National Natural Science Foundation of China (60874113), NSF-0242840, & NSF-0219110. This material is partly based on research sponsored by Air Force Research Laboratory under agreement number FA8750-10-2-0152 & the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The U.S. Government is authorized to reproduce and distribute reprints for Government purpose notwithstanding a copyright notation thereon. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College. We thank anonymous reviewers and Mehdi Azarmi for their good advice on improving our paper.

References

1. Bhargava B, Zhang Y, Idika N, Lilien L, et al. Collaborative attacks in WiMAX networks. *Security and Communication Networks* 2009; **2**(5): 373–391.
2. Bhargava B, Oliveira R, Zhang Y, et al. Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks. In *29th IEEE International Workshops on Distributed Computing Systems*, 2009, 447-450.
3. Sukwong O, Kim HS, Hoe JC. Commercial antivirus software effectiveness: an empirical study. *IEEE Computer* 2011; **44**(3): 63-70.
4. Zhou JS, Chen Z, Jiang W. Probability based IDS towards secure WMN. In *2010 2nd International Workshop on Intelligent Systems and Applications*, 2010, 1-4.
5. Garcia-Osorio A, Loo-Yau JR, Reynoso-Hernandez JA. A GaN class-F PA with 600 MHz bandwidth and 62.5% of PAE suitable for WiMAX frequencies. In *2010 IEEE International Microwave Workshop Series on RF Front-ends for Software Defined and Cognitive Radio Solutions* (*IMWS*), 2010,1-4.
6. Moore D, Paxson V, Savage S, et al. Inside the slammer worm. IEEE Security and Privacy 2003; **1**(4): 33–39.

7. Schuba CL, Krsul IV, Kuhn MG, et al. Analysis of a denial of service attack on TCP. In *IEEE Symposium on Security and Privacy*, 1997, 208-223.
8. Douceur J. The Sybil attack. In *the First International Workshop on Peer-to-Peer Systems*, 2002, 251-260.
9. Gong T, Li L, Du CX. Modeling and Simulation of Visual Tri-Tier Immune System. Applied Mechanics and Materials 2011; **48-49**: 701-704.
10. Robert MM. Viruses and Cancer—A Review. California Medicine 1965; **102**(5): 344–352.
11. Bordon Y. Mucosal immunology: Acid attack. Nature Reviews Immunology 2011; **11**: 156.
12. Gros P. In self-defense. Nature Structural and Molecular Biology 2011; **18**:401-402.
13. Ziv Y, Ron N, Butovsky O, et al. Immune cells contribute to the main- tenance of neurogenesis and spatial learning abilities in adulthood. Nature Neuroscience 2006; **9**: 268-275.
14. Gong T, Cai ZX. Anti-Worm Immunization of Web System Based on Normal model and BP Neural Network. Lecture Notes in Computer Science 2006; **3973**: 267-272.
15. Gong T, Cai ZX. Tri-tier Immune System in Anti-virus & Software Fault Diagnosis of Mobile Immune Robot Based on Normal Model. Journal of Intelligent and Robotic Systems 2008; **51**(2): 187–201.
16. Ramaswamy S, Fu H, Nygard K. Effect of cooperative blackhole attack on mobile ad hoc networks. In *ICWN*, 2005.
17. Wang W, Bhargava B, Lu Y, Wu X. Defending against wormhole attacks in mobile ad hoc networks. Wireless Communications and Mobile Computing 2006; **6**(4): 483–503.
18. McCune JM, Shi E, Perrig A, Reiter MK. Detection of denial-of-message attacks on sensor network broadcasts. In *Proc. IEEE Symposium on Security and Privacy*, 2005, 64-78.
19. Yu HF, Kaminsky M, Gibbons PB, et al. SybilGuard: defending against Sybil attacks via social networks. IEEE/ACM Transactions on Networking 2008; **16**(3): 576-589.
20. Maheshwari R, Gao J, Das SR. Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information, In *Proc. of the 26th Annual IEEE INFOCOM'07*, 2007, 107-115.
21. Cheung S, Lindqvist U, Fong M. Modeling multistep cyber attacks for scenario recognition. In *DARPA Information Survivability Conference and Exposition*, 2003, 1, 284-292.
22. Li X, Xu S. A stochastic modeling of coordinated internal and external attacks. *Technical Report*. 2007, Available at: http:// www.cs.utsa.edu/˜shxu/collaborative-attack-model.pdf
23. Yang J, Ning P, Wang XS, et al. CARDS: A distributed system for detecting coordinated attacks. In *Proc. of IFIP TC11 16th Annual Working Conference on Information Security*, 2000, 171-180.
24. Hussain A, Heidemann J, Papadopoulos C. COSSACK: coordinated suppression of simultaneous attacks. In *DISCEX*, 2003, 2, 94-96.
25. Ourston D, Matzner S, Stump W, et al. Coordinated internet attacks: responding to attack complexity. Journal of Computer Security 2004; **12**(2): 165–190.
26. Cuppens F, Miege A. Alert correlation in a cooperative intrusion detection framework. In *Proc. of IEEE Symposium on Security and Privacy, Toulouse*, 2002, 202-215.
27. Lin W, Xiang L, Pao D, Liu B. Collaborative Distributed Intrusion Detection System. In *2nd International*

Conference on Future Generation Communication and Networking, 2008, 1, 172-177.

28. Yu-Sung W, Foo B, Mei Y, Bagchi S. Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS. In *Proc. Computer Security Applications Conference*, 2003, 234-244.
29. Sarafijanovic S, Le Boudec JY. An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks. IEEE Transactions on Neural Networks 2005; **16**(5): 1076-1087.
30. Mohamed YA, Abdullah AB. Immune inspired framework for ad hoc network security. In *Proc. 2009 IEEE International Conference on Control and Automation*, 2009, 297-302.
31. Atakan B, Gulbahar B, Akan OB. Immune system-inspired evolutionary opportuni- stic spectrum access in cognitive radio ad hoc networks. In *Proceedings of 2010 The 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop*, 2010, 1-8.
32. IEEE Std 1074-2006 (Revision of IEEE Std 1074-1997). IEEE Standard for Developing a Software Project Life Cycle Process. 10.1109/ IEEESTD.2006.219190, 2006, 1-104.
33. Bau J, Mitchell JC. Security Modeling and Analysis. IEEE Security & Privacy 2011, **9**(3): 18-25.
34. Matzinger P. The danger model: a renewed sense of self. Science 2002, **12**: 301-305.
35. Motorola Inc. WiMAX security for real-world network service provider deployments. *White Paper*, 2007.
36. Shaked M, Shanthikumar J. *Stochastic Orders and Their Applications*. Academic Press, San Diego (CA), 1994.
37. Meltzoff A, Kuhl P, Movellan J, et al. Foundations for a New Science of Learning. Science 2009, **325**: 284-288.
38. Marchiori D, Warglien M. Predicting Human Interactive Learning by Regret-Driven Neural Networks. Science 2008, **319**: 1111-1113.
39. Edelman G. Learning in and from Brain-Based Devices. Science 2007, **318**: 1103-1105.
40. Behera L, Kumar S, Patnaik A. On Adaptive Learning Rate That Guarantees Conver- gence in Feed-forward Networks. IEEE Transactions on Neural Networks 2006, **17**(5): 1116 - 1125.
41. Kephart J. Learning from Nature. Science 2011, **331**: 682-683.
42. Breslau L, Estrin D, Fall K, et al. Advances in Network Simulation. IEEE Computer 2000, **33**(5): 59-67.