Novel Secure and Immune Private Routing Protocol in Mobile Ad Hoc Networks

Tao Gong, Bharat Bhargava, *Fellow, IEEE*, and Norman O. Ahmed

Abstract—The user anonymity is an important security factor to protect personal privacy in mobile ad hoc networks. Recently, Wu et al. proposed an ad hoc on-demand position-based private routing protocol (AO2P), but the AO2P is vulnerable to some collaborative attacks, such as blackhole & wormhole attacks. Once any compromised node is included in a route, it can conduct different attacks, which are very difficult to identify because of the pseudo identifiers in the AO2P. In order to immunize the mobile ad hoc networks against the collaborative attacks and enhance the security of the private routing protocol, a novel secure and immune private routing protocol is proposed and called as NSIPRP, in this paper. The NSIPRP is based on the native immunization of mobile nodes and the immune reconfiguration of the mobile ad hoc networks, and can be used to protect private information against the collaborative attacks. Analytical models are developed for evaluating the performances of the packet delivery ratio and the probability of routing failure. Analysis and simulation results show that, while the NSIPRP immunizes the mobile ad hoc networks against the collaborative attacks and preserves communication privacy in the mobile ad hoc networks, its routing performance is comparable with other position-based routing algorithms such as the AO2P.

Index Terms—Ad hoc routing protocol, security, communication privacy, immunization.

1 Introduction

THE user anonymity is becoming important to protect personal privacy in mobile ad hoc networks, because this approach makes it more difficult for adversaries to trace their potential victims and to attack them [1]. In routing protocols such as AODV [2], DSR [3], and DSDV [4], each node should disclose its identity (ID) to send or receive data via any route in the network, which makes the networks on theses protocols vulnerable against attacks and disruptions. To achieve communication anonymity, Wu et al. proposed a position-based ad hoc routing algorithm, named AO2P, which worked in the network with relatively high node densities and disclosed only the positions of destinations without the local position information exchange [1]. In the receiver contention mechanism of the AO2P, receiving nodes were divided into different classes according to how close they could bring the routing request toward the destination. Once a route was built, pseudo IDs and temporary MAC addresses were used for the nodes in the routes, so that communication anonymity could be achieved without disclosing the node identities. Eavesdroppers or attackers only knew that a node at a certain position would receive data, but they did not know the most accurate location of the node.

However, the AO2P is vulnerable to the collaborative attacks of the blackhole attacks and the wormhole attacks, which have camouflage abilities. The blackhole attack can transmit malicious broadcast information from a node that the node has the shortest path to the destination aiming to intercept messages [5]. The wormhole attacks can record packets at one location in the network, tunnel them to other locations to make pseudo shortest paths to the destinations, and retransmit them there into the network [6], [7]. So the wormhole attacks can make the normal nodes to send messages to the wormhole nodes, and they can also transform the normal nodes into new wormhole nodes. Therefore, the more normal nodes are infected, the more privacy information will be lost.

To defend against the collaborative attacks of the blackhole attacks and the wormhole attacks in the AO2P, a novel secure and immune private routing protocol, called as NSIPRP, is proposed. The NSIPRP is based on the AO2P, keeping the communication anonymity and disclosing only position information in the network for routing. Besides, the NSIPRP also has a normal-model-based defending mechanism against the collaborative attacks on each node, and it can detect learn and eliminate the collaborative attacks.

To deal with the collaborative attacks, IDS approaches were designed and used for matching the features of the attacks. Unfortunately these approaches are often ineffective to unknown attacks [8]. In fact, human immune network is an advanced natural defending system against unknown attacks from viruses, bacteria and cancer [9]. Thus, the biological immune network inspires us to design more advanced defense system against the unknown 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

- *T. Gong is with the College of Information Science and Technology, Donghua University, Shanghai 201620, China, and he is also a visiting scholar at the Department of Computer Science and CERIAS, Purdue University, West Lafayette, IN 47907, USA. E-mail: tgong@ purdue.edu.*
- *B. Bhargava is with the Department of Computer Science and CERIAS, Purdue University, West Lafayette, IN 47907, USA. E-mail: bb@ cs.purdue.edu.*
- *N.O. Ahmed is with the Department of Computer Science, Purdue University, West Lafayette, IN 47907, USA and he is also with the Air Force Research Laboratory. E-mail: ahmed24@ purdue.edu.*

Manuscript received 29 August 2011.

immune responses, the immune cells and immune molecules make up the parallel immune tier, which realize immune responses in parallel cells and molecules [10]. At first, the immune network against the attacks determines whether the strange objects are selfs and then detect the attacks [11]. 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 [12].

According to the bio-inspired ideas, an anti-worm static artificial immune system was proposed and evaluated based on the tri-tier immune model [13]. The immune model was also used in software fault diagnosis of mobile robots [14]. In this paper, the NSIPRP, which can detect the attacks, minimize the damages and keep the communication anonymity of the AO2P, was proposed and evaluated. The NSIPRP was designed against the collaborative attacks in the mobile ad hoc networks based on the AO2P and the immune model in section 2. In section 3, the detecting and learning capabilities of the NSIPRP were analyzed against the collaborative attacks. In section 4, the experiments of the NSIPRP-based secure immune network were implemented in the NS2 simulations, and the experimental results were compared with the AO2P-based ad hoc network against the collaborative attacks. Section 5 concluded the paper.

2 Related Research

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

Attacks in the mobile networks based on the IEEE 802.16j standard include blackhole attacks [15], wormhole attacks [6], denial-of-message attacks [16] and Sybil attacks [17] etc. Besides, the implementation bugs and the incompatibilities were also the potential sources of vulnerabilities [18].

To defend against these attacks, some 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 [19]. Li et al. built a stochastic model of collaborative internal and external attacks [20]. Yang et al. designed a signature-based model to detect collaborative attacks [21]. Based on multicast annotated topology information and blind detection techniques, Hussain et al. built a collaborative system to detect some distributed DoS attacks [22]. Ourston et al. used Hidden Markov models to detect attacks [23]. 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 [24]. 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 [25]. Yu-Sung et al. proposed a collaborative intrusion detection system, in which different types of IDSs worked cooperatively [26].

However, the above approaches are often ineffective to unknown collaborative attacks [8]. To overcome the disadvantages of the IDS approaches against the unknown attacks, the techniques of immune computation have been investigated for some security applications. Dasgupta et al. presented the technique inspired by the negative selection mechanism of the immune system that can detect foreign patterns in the non-self space [27]. In recent years, malicious computer software in the form of viruses and worms continues to plague modern information networks, so Balthrop et al. surveyed the structure of computer networks and analyze their epidemiological characteristics [28]. Esponda et al. proposed a formal framework to analyze the tradeoffs between positive and negative detection schemes in terms of the number of detectors needed to maximize coverage [29].

3 NSIPRP Routing Algorithm

In this section, a secure tri-tier immune model is built against the attacks for immunizing ad hoc routing algorithms. Based on the normal model of selfs (i.e. normal components of the artificial systems), the immune model and the AO2P, we then design the proposed anonymous routing algorithm, where the details on NSIPRP routing and immunization against the attacks are given. Next, we present a receiver classification scheme, followed with the receiver contention scheme and the defensive scheme. Based on these three schemes, the NSIPRP can process secure efficient route discovery. Finally, we design a software fault repairing algorithm to transform the abnormal attacked network into another normal one.

3.1 Secure Tri-tier Immune Model

We propose a secure tri-tier immune model for the mobile ad hoc networks against wormhole attacks in Fig. 1. The native immune tier is the first tier, which is used to detect the collaborative attacks mainly by detecting the selfs with the normal model, no matter whether the collaborative attacks are known or unknown for the network. The selfs are important for increasing detecting efficiency, and the normal model of the selfs is based on the space-time properties of the normal nodes. The second adaptive immune tier is used to learn the unknown attacks with the expendable multi-dimension feature space of attacks, when the wormhole attacks are unknown for the network. The immunization procedure of the secure immune model is described below.

First, the native immune tier detects the selfs, which are the normal components of a mobile ad hoc network, and the self model provides the space-time properties for the normal states to increase the precision of self detection as shown in Fig. 1. The self model and the self detection on the self model in the first step are important for the secure tri-tier immune model, because the self-based detection of compromised nodes is more accurate and efficient than the direct feature-matching detection of the

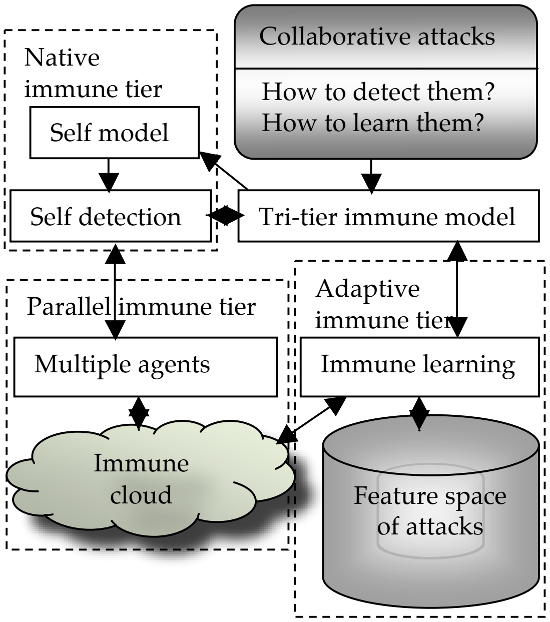

Fig. 1. Secure tri-tier immune model.

nodes. Moreover, when the self model is damaged, 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 Fig. 1. The immune cloud is a new parallel computing system, which is established in the cloud computing infrastructure and now used to increase the efficiency and robustness of immune computation. In Fig. 1, the immune learning is made by searching the most similar known attacks in the feature space of attacks.

After any attack in the collaborative attacks is detected at any part of the mobile ad hoc network, the information about the attacked node will be sent to the relative immune tier to activate the immune responses against the attack. Afterwards, the attack that has been detected will be recognized by matching their available features in the expendable feature space of all the known blackhole attacks and wormhole attacks with the real-time searching algorithms. If the search result has at least one correct record, then the collaborative attack will be controlled and cleared in a relatively easy way, and both the features and the research result of the collaborative attack will be delivered to the relative immune tier to eliminate the collaborative attack, keeping the mobile ad hoc network secure. If the search result returns nothing, then the collaborative attack as an unknown object will be learnt with some intelligent methods such as enhanced learning from examples and learning based on neural network etc. The immune learning is partly built on the cloud computing and the learning process should be finished in real time. The learning in the brain and the brain-based devices discover unknown knowledge by comparing the unknown objects with the known objects and testing the unknown ones [31], [32], [33], [34]. To recognize the unknown attacks, the immune learning algorithm first acquires the feature information of the attacked node, and then it transforms the feature data of the unknown attack into a point in the feature space of attacks, which is built with the feature information of all the known attacks. Then the algorithm searches the best suitable class for the unknown attack, which is the class of the most similar known attack to the unknown one. The searching procedure is random and optimal, and the immune learning algorithm can be built on the evolutionary search or non-evolutionary heuristic search. After the search returns a optimal solution, the most similar known attack to the unknown one is found. So the type and processing solution for the unknown attack can be calculated with the type of the most similar known attack and both the feature information of the unknown attack and the most similar known attack. Through this immune learning based on memory, the unknown attack can be turned into a new known attack in the feature space of attacks.

3.2 NSIPRP Routing Protocol Based on AO2P

In AO2P-based NSIPRP, a source discovers the route through the delivery of a routing request to its destination and the attack detection of candidate next node based on the normal model of selfs in the node and immune model. A node en-route from one normal node to another normal node will generate a pseudo node ID and a temporary MAC address. Once a route is built up, data is forwarded from the source to the destination based on the pseudo IDs and the immune detection mechanism. Once a compromised node is detected with the immunization on the normal model, the node should be under some attacks and will be repaired by recovering the compromised node after eliminating the attacks. This section gives the details on AO2P-based routing discovery with immunity. Other issues, such as immune detection and secure data delivery with immunity, are addressed in section 4.

Once a source needs to find the route to its destination, it first generates a pseudo ID and a temporary MAC address for itself through a globally defined hash function using its position and the current time as the inputs [1]. Because of the space-time unique identification, such a procedure makes the probability that two nodes involved in routing have the same ID and MAC address small and negligible. The source then sends out a routing request (*rreq*) message. The *rreq* message carries the information needed for routing, such as the position of the destination and the source's pseudo ID.

The neighboring nodes around the source, called receivers, should be detected by the native immune tiers of the receivers before the receivers receive the *rreq*. If a receiver is determined as a non-compromised one by the immune detection and the receiver is the destination, the connection between the source and the destination will be confirmed by more messages. If the receive is compromised, the receiver will be isolated by the immune tier so that the source will not send the *rreq* message to the compromised node until the node has been repaired well. At the same time, another receiver will be checked to expand the route until the destination is found in the end. If the receiver is a non-compromised one and is not the destination yet, the receiver will assign itself to a receiver class following the rules for classifying nodes based on the po-

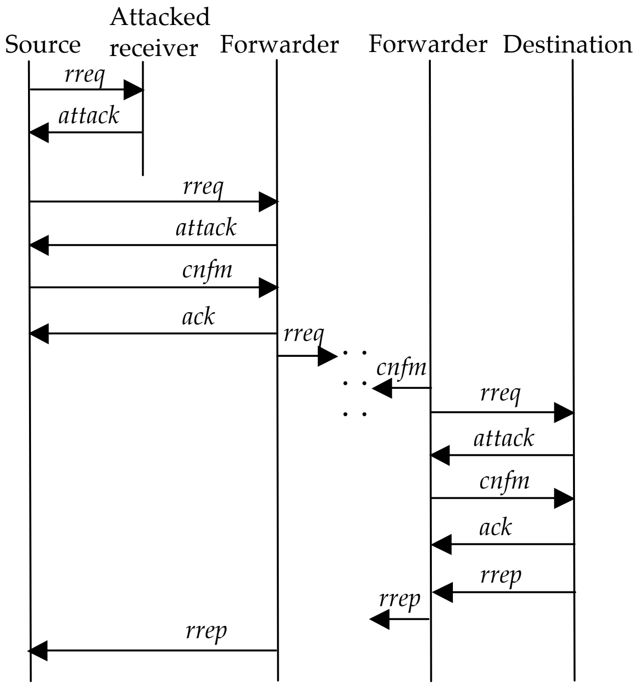

Fig. 2. Message flow in AO2P-based NSIPRP routing discovery.

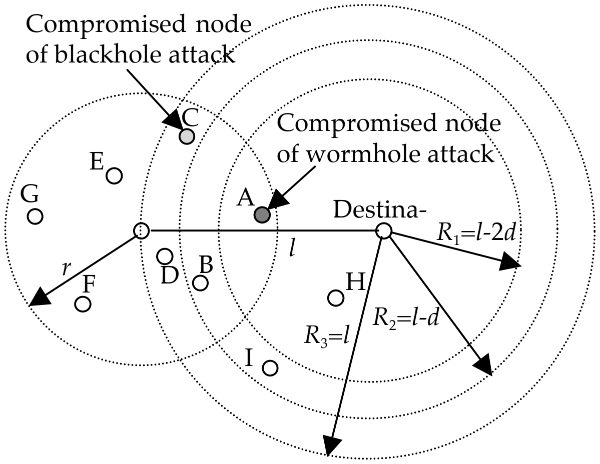
Compromised node of blackhole attack
C
Compromised node of wormhole attack
E
G
A
Destina-
R_1=l-2d
l
r
D
B
F
H
R_2=l-d
R_3=l
I

Fig. 3. Classifying nodes based on the positions and the immune detection against the attacks.

sitions [1] and the immune detection against the attacks. Each non-compromised receiver uses the hash function to generate a pseudo ID and a temporary MAC address. The inputs of the hash function are the receiver's position and the time it receives the *rreq*. If any receiver is compromised due to the collaborative attacks, the receiver will have no pseudo ID or temporary MAC so that the attacks on the receiver can be easier to detect and eliminated than those with the pseudo ID and the temporary MAC.

The receivers then contend for the wireless channel to send out hop reply (*hrep*) messages in a so-called rreq contention phase [1]. The receiver that has successfully sent out the *hrep* will be the next hop. If the receiver is compromised because of the attacks, the immune tier of the receiver will send back an *attack* message to the source, as shown in Fig. 2. After the compromised receiver has been repaired, the immune tier of the receiver will send back a *repaired* message to the source so that the source can send the *rreq* message to the repaired receiver again.

On receiving the hrep, the source replies with a message of confirming (*cnfm*), and then the next hop of the source replies to this message with an *ack*. Upon receiving the *ack*, the source saves the pseudo ID and the temporary MAC address of the next hop in its routing table.

After receiving the *cnfm*, the next-hop receiver becomes a sender, which is defined as the source or an intermediate node to forward the *rreq* message. Once the sender receives a *hrep*, it couples the pseudo ID and the temporary MAC address of its next hop with those of its previous hop and saves the pairs in the routing table.

The searching of the next hop is repeated until the destination receives the *rreq*. After receiving the cnfm from its previous hop, the destination sends a routing reply (*rrep*) message through the reverse path to the source. The message flow in AO2P-based NSIPRP routing discovery is shown in Fig. 2, and the frames for important control messages are shown in Fig. 3.

A route discovery failure will occur when a sender cannot find a legitimate next hop. Routing discovery failure may also be caused due to destination mobility and/or the collaborative attacks. In these cases, a routing discovery failure report will be sent back to the source. The source will start a new route search based on the destination's most updated position after the compromised nodes in the route have been repaired.

A simple illustrated example of node classification is shown in Fig. 3, based on the attack detection with the native immunization. A distance of d is calculated as $d = r/3$, where r is the maximum radio coverage of the ad hoc channel. The nodes (e.g., node A), which fall into the circle centered at the destination with a radius of l-2d, belong to class 1 that has the highest priority. But node A is infected by the wormhole attack so that another node should be chosen as the next hop of the sender. The nodes (e.g., node B), which fall between the two circles centered at the destination with the radiuses of l-d and l-2d respectively, belong to class 2 that has lower priority than class 1. The nodes (e.g., node C and D), which fall between the two circles centered at the destination with the radiuses of l and l-d respectively, belong to class 3 that has lower priority than class 2. Node C is infected by the blackhole attack, and this node cannot be chosen as the next hop of the sender before the node has been repaired. For nodes E, F, and G, they belong to class 4 and will lead the rreq away from the destination. Other nodes, such as H and I, are out of the sender's transmission range and cannot receive the *rreq*.

4 NSIPRP Performance Evaluation

In NSIPRP, a hop reply (*hrep*) contention period may cause extra delay in the route discovery, and the immune detection of the compromised nodes will cause inevitable delay too. If such a delay is large, a routing failure or a route discovery failure may occur because the destination may be out of reach or compromised by the collaborative attacks. A route discovery failure may also be caused by inaccurate position information or the network topology where a next hop cannot be found. In this section, the probability for detecting the collaborative attacks is analyzed at first. Based on the immune detection, the hrep average delay and the average time needed for a successful next hop determination are calculated. Lastly, the probability of a route discovery failure is analyzed under different node distribution and position accuracy. The definitions of major symbols used in the following analysis are listed in Table 1.

4.1 Probability for NSIPRP Immune Detection

Suppose a mobile ad hoc network is represented as finite immune graph $G=(V, E)$, where V is the node set, and E is the edge set with $E \neq \phi$. Any element in the set V is a node in the mobile ad hoc network, and any element in the set E represents the relationship between one node 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 non-compromised, and the non-compromised state is identified by the space-time representation of its normal model [9]. It is 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 in a sequential order, a node is secure, compromised, or removed at any point in time. When a node is compromised by the attacks, it may attack other nodes as a new tool of the attackers. The attacks may remove crucial nodes in the topology path of the mobile network, and the compromised nodes may be removed in its immune response in order to be repaired by its backup ones.

Suppose D_t, $N(t)$ and $M(t)$ respectively denote the set of the nodes that are compromised by the attacks at the time no later than t, the sum of the nodes that are compromised the attacks at the time no later than t, and the sum of the nodes that are removed or lost at the time no later than t. Therefore, $N(t)$-$M(t)$ denotes the sum of the nodes that are compromised but have not been removed by the time t. For the event that the node was compromised, 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 compromised (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 compromised by the attacks at time T_k, i.e. the kth compromised node, is denoted by node(T_k). Suppose for any sequence of compromised 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 [20].

For random variables R_1 and 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 $R_1 \succeq_{st} R_2$ [30]. 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 [20]:

$$S_i \succeq_{st} S_{i+1},\ i = 0,1,\cdots,|V|-1. \tag{1}$$

This proposition is used to prove that the coordinated attacks become more powerful as more internal nodes are compromised and produce new attacks. Here, the discretization makes T_k follows a discrete Poisson process of success probabilities r_{k-1} for k= 1, …, $|V|$ [20], and the probabilities r_{k-1} are denoted by the following formula:

$$\begin{aligned} r_i &= \frac{|V| + d_1 + d_2 + \cdots + d_i - i}{2|E| + |V|} \\ r_0 &= \frac{|V|}{2|E| + |V|},\ i = 1,2,\cdots,|V|-1 \end{aligned}, \tag{2}$$

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

After the compromised node node(T_i) is detected, the node should be isolated immediately by cutting off the compromised node's output. It is assumed that the success probability of detecting the compromised node is denoted by p_i and so the success probability of cutting off the output of the compromised node equals to p_i. Therefore, according to (2), the probability r_i with detection is improved by the following formula:

$$\begin{aligned} r_i &= \frac{|V| + \sum_{j=1}^{i-1} d_j + d_i \cdot (1 - p_i) - i + 1 - p_i}{2|E| + |V|} \\ &= \frac{|V| + \sum_{j=1}^{i} d_j - p_i \cdot (d_i + 1) - i + 1}{2|E| + |V|} \end{aligned}, \tag{3}$$

In general, there are 3 strategies to find the compromised node: (1) attack detection directly by getting and matching the features of the compromised 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 compromised by the known attacks, then the success probability $p_i^{(1)}$ for strategy 1 can be denoted by the following formula:

$$p_i^{(1)} = \frac{|F_B|}{|F_A|} \cdot p_e^{(1)},\ i = 1,\cdots,|V|, \tag{4}$$

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:

$$p_i^{(2)} = p_l \cdot p_e^{(2)},\ i = 1,\cdots,|V|, \tag{5}$$

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:

TABLE 1
MATHEMATICAL SYMBOLS USED IN THE ANALYSIS

Symbol	Meaning
G	Finite immune graph for mobile ad hoc network, G=(V, E), where V is the node set, and E is the edge set
$N(t)$	Sum of the nodes that are compromised by the attacks at the time no later than t
$M(t)$	Sum of the nodes that are removed or lost at the time no later than t
D_i	Distribution that the degree of node(T_i) follows, and is distributed as the degree distribution D of G
i_{SYNC}	Time duration for synchronization interval
i_{PS}	Time duration for a prioritization slot
i_{ES}	Time duration for a elimination slot
i_{YS}	Time duration for a yield slot
i_{rreq}	Time duration for *rreq*
i_{hrep}	Time duration for *hrep*
i_{cnfm}	Time duration for *cnfm*
i_{ack}	Time duration for *ack*
i_{SIFS}	Time duration for *SIFS*, which is a short inter-frame space message exchange
$t_A(n)$	Time duration for detecting the compromised nodes before finding an available node among n contenders
$P_T(n)$	Probability of a successful *hrep* attempt among n contenders
$P_F(n)$	Probability of a failed *hrep* attempt among the available nodes of n contenders
$P_A(n)$	Probability of an attack detection attempt among n contenders
$\overline{B}_E(n)$	Average number of bursts in elimination phase when n receivers are in *hrep* contention
$\overline{L}_Y(n)$	Average number of yield slots in a successful attempt when n receivers are in *hrep* contention
$\overline{L'}_Y(n)$	Average number of yield slots in a failed attempt when n receivers are in *hrep* contention
$\overline{D}_T(n)$	Average time for a successful *hrep* transmission cycle
$\overline{D}_{RT}(n)$	Average time for a failed *hrep* transmission cycle
$\overline{D}_{REQ}(n)$	Average time for next hop determination when there are initially n contenders

$$p_i^{(1)} \le p_i^{(2)}, \tag{6}$$

$$r_i^{(1)} \ge r_i^{(2)}. \tag{7}$$

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 compromised 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, and the following experience formula is mostly correct:

$$0 = \frac{|F_B|}{|F_A|} < p_l \le 0.8\,. \tag{8}$$

Thus, (6) and (7) 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 compromised by the known attacks or not, the success probability $p_i^{(3)}$ for strategy 3 can be denoted by the following formula:

$$p_i^{(3)} = p_s \cdot p_e^{(3)},\ i = 1,\cdots,|V|, \tag{9}$$

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 compromised by known attacks,

$$p_i^{(3)} \approx p_i^{(2)} \ge p_i^{(1)}, \tag{10}$$

$$r_i^{(3)} \approx r_i^{(2)} \le r_i^{(1)}. \tag{11}$$

But, when the node is compromised by some unknown attacks, according to (8), the following formulas are correct.

$$1 = p_S > 0.8 \ge p_l > \frac{|F_B|}{|F_A|} = 0\,. \tag{12}$$

$$\therefore\ p_S \cdot p_\varepsilon^{(3)} > p_l \cdot p_\varepsilon^{(2)} > \frac{|F_B|}{|F_A|} \cdot p_\varepsilon^{(1)}. \tag{13}$$

$$\therefore p_i^{(3)} > p_i^{(2)} > p_i^{(1)}, \tag{14}$$

$$\therefore r_i^{(3)} < r_i^{(2)} < r_i^{(1)}. \tag{15}$$

In summary, for any attack, the following formula is correct.

$$r_i^{(3)} \le r_i^{(2)} \le r_i^{(1)}. \tag{16}$$

For $\gamma \in \{1,2,3\}$, the time at which the kth incident due to attacks occurs for detection strategy γ is denoted by $T_k^{(\gamma)}$ [20], then for k=1, 2, …, | V |, the theorem below is correct:

$$T_k^{(3)} \ge T_k^{(2)} \ge T_k^{(1)}. \tag{17}$$

The above reasoning shows that detection strategy 3 outperforms detection strategy 2 and detection strategy 1 to fight against the attacks. In general, some of the collaborative attacks are known and the others are often unknown. So if the space-time property set F_S is of 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.

4.2 Delay for NSIPRP Next Hop Searching

Though a network with relatively high node density is considered for the simplicity of analysis, neighbors belonging to the class with the highest priority are not always available due to the collaborative attacks. Thus, in the *hrep* prioritization phase, if all the relative nodes with the candidate route are all without any attack, the delay is approximately the time duration for two slots: the destination acknowledgement slot and the slot for the class with the highest priority. Otherwise, the delay should also include the time for the immune tier to detect the compromised neighboring nodes before finding an available neighboring node, and the detection time depends on the attack detection approach and the complexity of the collaborative attacks.

Suppose there are initially n contenders, the average time $\overline{D}_{REQ}(n)$ for next hop determination is calculated. It is assumed that n receivers belong to the class with the highest priority and will enter the elimination phase upon receiving a message of *rreq*. It is also assumed that a sender has to send the *rreq* k times before it receives a *hrep* successfully. The average delay for a sender to determines its next hop when there are n neighboring nodes contending to be the next hop can be calculated below:

$$\overline{D}_{REQ}(n) = t_S(n) + \frac{P_F(n)}{P_T(n)} t_F(n) + \frac{P_A(n)}{P_T(n)} t_A(n)\,. \tag{18}$$

$$P_A(n) = 1 - P_T(n) - P_F(n) \tag{19}$$

Here, the following can be calculated according to [1]:

$$t_S(n) = i_{rreq} + \overline{D}_T(n) + i_{hrep} + i_{SIFS} + i_{cnfm} + i_{SIFS} + i_{ack}\,, \tag{20}$$

$$\overline{D}_T(n) = i_{SYNC} + 2i_{PS} + \overline{B}_E(n)i_{ES} + \overline{L}_Y(n)i_{YS} + i_{ES}\,, \tag{21}$$

$$t_F(n) = i_{rreq} + \overline{D}_{RT}(n) + i_{hrep} + i_{SIFS}\,, \tag{22}$$

$$\overline{D}_{RT}(n) = i_{SYNC} + 2i_{PS} + \overline{B}_E(n)i_{ES} + \overline{L'}_Y(n)i_{YS} + i_{ES}\,, \tag{23}$$

Our observations and the data with some sample values for various parameters are given in Section 5.

4.3 Routing Failure and Impact of Collaborative Attacks

In the AO2P-based NSIPRP, the position error at senders or receivers may make the receivers assign themselves to the wrong classes [1]. However, position errors will not cause a routing failure by generating the links that actually do not exist, and the connection between a sender and a receiver without any attack thus is always real regardless of wrong positions. But, if a receiver is compromised by the collaborative attacks, the connection between the sender and receiver should be forbidden until the receiver is repaired. Moreover, the damages of the receivers can cause the incompleteness of the network functions and so increase the probability of a failed *hrep* attempt among the available nodes of n contenders.

When the receiver is compromised, the necessary disconnection between the sender and the receiver causes a routing failure from the sender. Thus, the probability of routing failure in the NSIPRP, denoted as $P_{RF}(n)$, is calculated below:

$$P_{RF}(n) = P_A(n) + P_F(n) = 1 - P_T(n) \tag{24}$$

When the collaborative attacks exist, the probability of

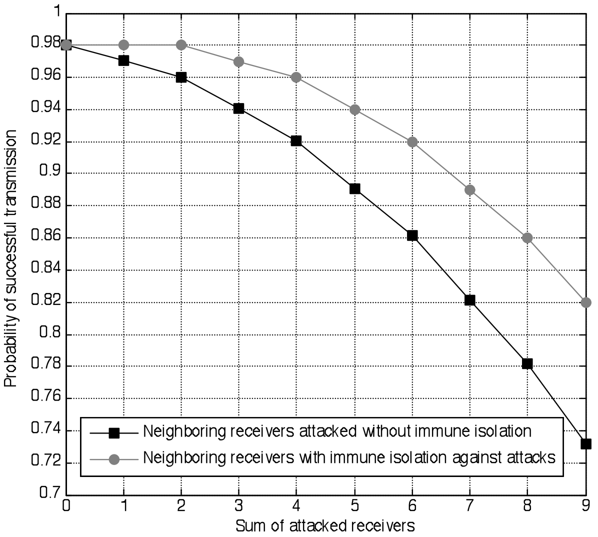

Fig. 4. Probability for successful *hrep* transmission under attacks.

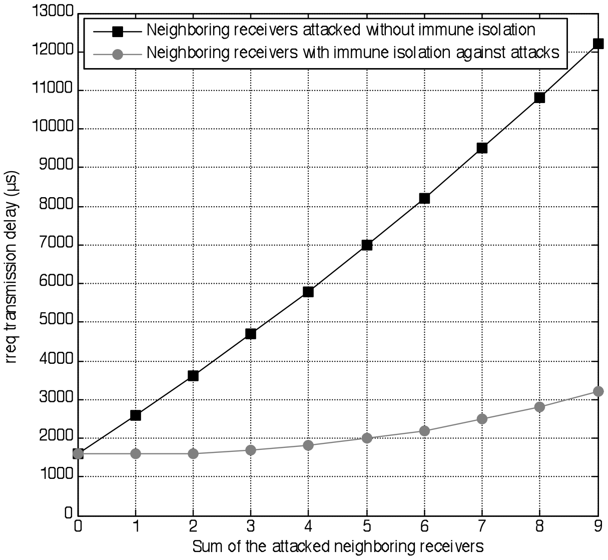

Fig. 5. Average time to determine a next hop under attacks.

$P_A(n)$ can increase and the probability of $P_F(n)$ will also increase. Thus, the probability of $P_F(n)$ will decrease until the collaborative attacks are eliminated by the immune tiers. After the compromised receivers have been repaired by the immune tiers, the probability of routing failure in the NSIPRP will be changed below:

$$P_{RF}(n) = P_F(n) = 1 - P_T(n) \qquad (25)$$

Therefore, the immunization mechanism is useful for decreasing the probability of $P_{RF}(n)$ and then increasing the probability of $P_T(n)$.

5 Illustrative Data and Observations

In this section, both analysis and simulation studies are presented. First, the analytical results on route discovery delay and the probability of a failure in route discovery are presented in the mobile ad hoc network under the collaborative attacks and the immune mobile ad hoc network against the attacks. Then a simulation model is used to study the data packet delivery ratio and the probability of a route discovery failure under destination mobility and the collaborative attacks.

5.1 Analysis Results

The parameters in an AO2P-based NSIPRP *hrep* contention period are set the same as those in AO2P [1]. Time duration for the synchronization interval is 11 μs, and time duration for SIFS is 28 μs as that in WLAN. The messages *rreq*, *hrep*, and *cnfm* are transmitted at the rate of 1 Mb/s. The message *ack* has an overall length of 240 bits and is also transmitted at the rate of 1 Mb/s. Time duration for the native immune tier to detect the attack on one receiver is 1*s* in average time for simplification of the analysis.

Fig. 4 shows the probability of a successful *hrep* transmission from the sender to *s* non-compromised receivers among *n* neighboring receivers. It shows that, when *m* (*m*=*n*-*s*), the sum of the compromised nodes among *n* neighboring receivers without isolating the compromised receivers by the immune tiers, increases, the probability for a successful hrep transmission decreases faster than that of the neighboring receivers with isolating the compromised receivers by the immune tiers against the attacks. When *m* equals to 0, the probability of a successful *hrep* transmission is the best. When *m* equals to *n*, the probability of a successful *hrep* transmission will be the worst, i.e. 0.

The corresponding average delay for a node to determine its next hop (i.e., the average time for the completion of *rreq* transmission cycle) is shown in Fig. 5. As the curves of the delays show, a higher transmission probability results in a lower next hop searching delay, while more attacks results in a higher next hop searching delay. Moreover, the immune tier against the attacks can restrain the increase of the next hop searching delay, so that the next hop searching delay of isolating the compromised neighboring receivers with the immune tiers increases more slowly than that of the neighboring receivers under attacks without immune isolation.

5.2 Simulation Results

The simulation scenario is a network covering an area of $1{,}000\, m \times 1{,}000\, m$, where a number of nodes are uniformly deployed. The transmission range for the ad hoc channel is 250*m*. The receivers are divided into 4 classes according to the rules in Section 3.2. To avoid disturbances from the warm-up period, the first 2 seconds of the simulation results were excluded. NS2 is used as the simulator, because it has the well-developed mobile ad hoc network model. The almost same simulation parameters are used in the NSIPRP-based network as that of the AO2P-based network [1], as shown in Table 2.

Fig. 6 shows the varying probability of a routing failure in NSIPRP as some neighboring receivers of the mobile ad hoc network are attacked and immunized. The x-axis is the reaction time of the simulation, and the col-

TABLE 2
PARAMETER SETTING OF NS2-BASED EXPERIMENTS

Parameter name	Setting value
Simulation time	10 s
Number of nodes	8
Transmission range	25 m
Topology	1,000 $m \times$ 1,000 m
Traffic	CBR
Normal packet size	512 bytes
Abnormal packet size	1024 bytes
Data rates	1 Mb/s

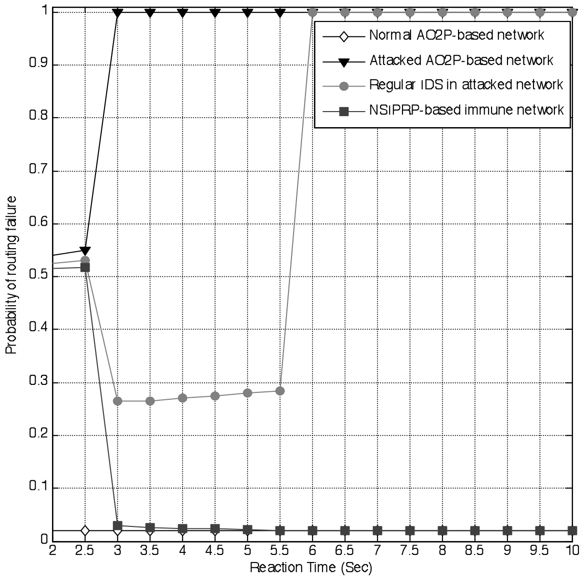

Fig. 6. Probability of routing failure under attacks with immunization.

laborative attacks are of the wormhole attacks and the blackhole attacks. In the simulation, the probability of routing failure in the normal mobile ad hoc network is kept the lowest, i.e. 0.02. Unfortunately, the collaborative attacks obviously increase the probability of routing failure in the network, and then the probability becomes 1 especially when the wormhole attacks spread all over the network. Though the regular IDS approach can detect the known blackhole attack and decrease the probability of routing failure in the attacked network from 3*s* to 6*s* in Fig. 6, the probability of routing failure increases obviously from 6*s* to 10*s* because the spread of the unknown wormhole attacks conquered the whole network in the end. At the time that all the nodes of the network are infected by the wormhole attacks, the private information on the nodes is easier to steal by the attackers even if the information is encrypted. Fortunately, the NSIPRP-based immune network can work strongly against the collaborative attacks and decrease the probability of routing failure in the attacked network to the normal value.

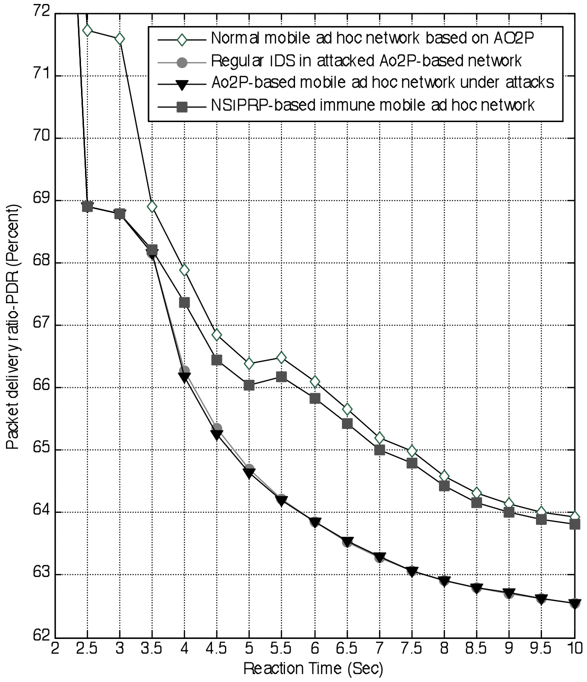

Fig. 7. Data packet delivery ratio in AO2P-based mobile ad hoc network on different conditions of attacks and immunization.

Fig. 7 compares the simulated delivery ratio in the networks on the different conditions of the collaborative attacks and the NSIPRP-based immunization. It shows that, generally, the normal AO2P-based mobile ad hoc network has the highest delivery ratio as it is not attacked at all. The attacked AO2P-based network without any defensive mechanism has the lowest delivery ratio. The regular IDS approach can deal with the known attack and increase the delivery ratio from 3I to 6*s*. But some unknown attacks can conquer the AO2P-based network with IDS, and the delivery ratio decreases to the lowest in the end. The NSIPRP-based immunization approach is effective for the mobile ad hoc network against the collaborative attacks, and the delivery ratio increases to the highest after the immunization is activated.

6 CONCLUSIONS AND FUTURE WORKS

This research proposes a novel routing algorithm, named NSIPRP, to improve the AO2P algorithm in the mobile ad hoc networks against the collaborative attacks. The secure tri-tier immune model is used for attack detection during the process of route discovery. Only non-compromised receivers are used for the next hop selection of the senders, and the compromised receivers are isolated and immunized. After the infected receivers have been repaired, they can be used as non-compromised ones. We use analysis and simulation to evaluate the routing performance for the proposed algorithm against the collaborative attacks.

When the mobile ad hoc network is attacked and immunized, the extra *rreq* transmission delays are caused by the detection of the compromised receivers according to an analytical model. The delay is smaller than that of the failure caused by the collaborative attacks in the whole network.

In the network layer, some analysis and simulations are used to evaluate the impact of the collaborative attacks and the NSIPRP-based immunization on route discovery. It is observed that the collaborative attacks may cause inefficient routing and route failure. But the NSIPRP-based immunization can restrain the damages of the collaborative attacks and repair the compromised nodes in the network. Finally, we compare the routing performance of the normal AO2P-based network, the AO2P-based network under the collaborative attacks, and the NSIPRP-based immune network. The simulation shows that the NSIPRP-based immunization can quickly increase the delivery ratio to reach the normal value, while the regular IDS approach can only increase little delivery ratio and then decrease to the lowest value because of the unknown attacks in the end.

We propose the following two future research directions:

- **Network reconfiguration for protecting privacy.** Internal attackers are able to attack the most important nodes or the most frangible parts of the network. The intelligent reconfiguration of the attacked network will increase the complexity and difficulty for the attackers to steal the privacy information. Future work will include building the immune reconfiguration model for the attacked network to protect the privacy information and improve the security of the network.
- **Expanded immune learning of unknown attacks.** Current learning mechanism is based on the fixed dimensions of the feature space, and in fact the feature dimensions of unknown attacks are expandable. Because the attacks are designed by intelligent programmers, the programmers can learn to create new feature dimensions to make the attacks more complex and harder to detect. Future work will emphasize on building a novel immune learning model to expand the feature dimensions of unknown attacks adaptively, so that the immune network will have greater power to detect and eliminate more complex unknown attacks.

ACKNOWLEDGMENT

The work was supported in part by grants from the National Natural Science Foundation of China (60874113), Natural Science Foundation of Shanghai (08ZR1400400), and the Shanghai Educational Development Foundation (2007CG42), NSF-0242840, NSF-0219110. This material is partly based on research sponsored by Air Force Research Laboratory under agreement number FA8750-10-2-0152 and 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 for their good advice on improving our paper.

REFERENCES

[1] X.X. Wu and B. Bhargava, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” *IEEE Transactions on Mobile Computing*, vol. 4, no. 4, pp. 335-348, July/August 2005, doi: 10.1109/TMC.2005.50.

[2] C.E. Perkins and E.M. Royer, “Ad-Hoc On-Demand Distance Vector Routing,” *Proc. Second IEEE Workshop Mobile Computing Systems and Applications*, pp. 90-100, 1999.

[3] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” *Proc. ACM SIGCOMM-Computer Comm. Review*, pp.153-181, 1996.

[4] C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers,” *Proc. ACM SIGCOMM*, pp. 234-244, 1994.

[5] Ramaswamy S, Fu H, Nygard K. Effect of cooperative blackhole attack on mobile ad hoc networks. In ICWN, 2005.

[6] W. Wang, B. Bhargava, and Y. Lu, et al, “Defending against wormhole attacks in mobile ad hoc networks,” *Wireless Communications and Mobile Computing*. vol. 6, no. 4, pp. 483-503, June 2006.

[7] R. Maheshwari, J. Gao, and S. R. Das, “Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information,” *Proc. of the 26th Annual IEEE INFOCOM’07*, pp. 107-115, 2007.

[8] O. Sukwong, H.S. Kim, and J.C. Hoe, “Commercial antivirus software effectiveness: an empirical study,” *IEEE Computer*, vol. 44, no. 3, pp. 63-70, March 2011.

[9] T. Gong, L. Li, and C.X. Du, “Modeling and Simulation of Visual Tri-Tier Immune System,” *Applied Mechanics and Materials*, vol. 48-49, pp. 701-704, February 2011.

[10] Y. Bordon, “Mucosal immunology: Acid attack,” *Nature Reviews Immunology*, vol. 11, pp. 156, March 2011.

[11] P. Gros, “In self-defense,” *Nature Structural and Molecular Biology*, vol. 18, pp. 401-402, February 2011.

[12] Y. Ziv, N. Ron, and O. Butovsky, et al, “Immune cells contribute to the maintenance of neurogenesis and spatial learning abilities in adulthood,” *Nature Neuroscience*, vol. 9, pp. 268-275, January 2006.

[13] T. Gong and Z.X.Cai, “Anti-Worm Immunization of Web System Based on Normal model and BP Neural Network,” *Lecture*

Notes in Computer Science, vol. 3973, pp. 267-272, May 2006.

[14] T. Gong and Z.X. Cai, "Tri-tier Immune System in Anti-virus and Software Fault Diagnosis of Mobile Immune Robot Based on Normal Model," *Journal of Intelligent and Robotic Systems*, vol. 51, no. 2, pp. 187–201, February 2008.

[15] M. Al-Shurman, S.M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," *Proceedings of the 42nd annual Southeast regional conference*, pp. 96-97, 2004.

[16] J.M. McCune, E. Shi, and A. Perrig, et al, "Detection of denial-of-message attacks on sensor network broadcasts," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 64-78, 2005.

[17] H. Yu, M. Kaminsky, and P.B. Gibbons, et al, "SybilGuard: defending against Sybil attacks via social networks," *Proceedings of ACM SIGCOMM*, pp. 267-278, 2006.

[18] B. Bhargava, Y. Zhang, and N. Idika, et al, "Collaborative attacks in WiMAX networks," *Security and Communication Networks*, vol. 2, no. 5, pp. 373-391, 2009.

[19] S. Cheung, U. Lindqvist, and M. Fong, "Modeling multistep cyber attacks for scenario recognition," *Proceedings of DARPA Information Survivability Conference and Exposition*, pp. 284-292, 2003.

[20] X. Li, S. Xu, "A stochastic modeling of coordinated internal and external attacks," *Technical Report*, http://www.cs.utsa.edu /~shxu/collaborative-attack-model.pdf. 2007.

[21] J. Yang, P. Ning, and X.S. Wang, et al, "CARDS: A distributed system for detecting coordinated attacks," *Proceedings of IFIP TC11 16th Annual Working Conference on Information Security*, pp. 171-180, 2000.

[22] A. Hussain, J. Heidemann, and C. Papadopoulos, "COSSACK: coordinated suppression of simultaneous attacks," *Proceedings of DISCEX*, pp. 2-13, 2003.

[23] D. Ourston, S. Matzner, and W. Stump, et al, "Coordinated internet attacks: responding to attack complexity," *Journal of Computer Security*, vol. 12, no. 2, pp. 165-190, April 2004.

[24] F. Cuppens and A. Miege, "Alert correlation in a cooperative intrusion detection framework," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 202-215, 2002.

[25] W. Lin, L. Xiang, and D. Pao, et al, "Collaborative Distributed Intrusion Detection System," *Proceedings of 2nd International Conference on Future Generation Communication and Networking*, pp. 172-177, 2008.

[26] W. Yu-Sung, B. Foo, and Y. Mei, et al, "Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS," *Proceedings of Computer Security Applications Conference*, pp. 234-244, 2003.

[27] D. Dasgupta and F. González, "An immunity-based technique to characterize intrusions in computer networks," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 3, pp. 281-291, 2002.

[28] J. Balthrop, S. Forrest, and M.E.J. Newman, et al, "Technological Networks and the Spread of Computer Viruses," *Science*, vol. 304, no. 5670, pp. 527-529, 2004.

[29] F. Esponda, S. Forrest, and P. Helman, "A formal framework for positive and negative detection," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 34, no. 1, pp. 357-373, 2004.

[30] M. Shaked and J. Shanthikumar, *Stochastic Orders and Their Applications*. San Diego, Calif.: Academic Press, 1994.

[31] A. Meltzoff, P. Kuhl, and J. Movellan, et al, "Foundations for a New Science of Learning," *Science*, vol. 325, pp. 284-288, 2009.

[32] D. Marchiori and M. Warglien, "Predicting Human Interactive Learning by Regret-Driven Neural Networks," *Science*, vol. 319, pp. 1111-1113, 2008.

[33] G. Edelman, "Learning in and from Brain-Based Devices," *Science*, vol. 318, pp. 1103- 1105, 2007.

[34] L. Behera, S. Kumar, and A. Patnaik, "On Adaptive Learning Rate That Guarantees Convergence in Feed-forward Networks," IEEE Transactions on Neural Networks, vol. 17, no. 5, pp. 1116-1125, 2006.

Tao Gong received the BS degree in Mathematics from the Hunan University of Science and Technology in 2000 and the MS degree in Pattern Recognition and Intelligent Systems and PhD degree in Computer Science from the Central South University respectively in 2003 and 2007. He is an associate professor of computer sciences at Donghua University, China, and he is also a visiting scholar at Department of Computer Science and CERIAS, Purdue University. He is the General Editors-in-Chief of the first leading journal *Immune Computation* in its field, and an editorial board member of some international journals such as Journal of Computers in Mathematics and Science Teaching, International Journal of Security and Its Applications, and International Journal of Multimedia and Ubiquitous Engineering. He is also a program committee member of some international conferences such as IEEE ICNC 2011, IEEE BMEI 2011, and WMSE 2011 etc. He is a Life Member of Sigma Xi, The Scientific Research Society, and has been granted with Chen Guang Scholar of Shanghai. His research has been supported by National Natural Science Foundation of China, Shanghai Natural Science Foundation and Shanghai Educational Development Foundation etc. He has published over 60 papers in referred journals and international conferences, and over 20 books such as *Artificial Immune System Based on Normal Model and Its Applications*, and *Advanced Expert Systems: Principles*, *Design and Applications* etc. His current research interests include network security, security in mobile embedded systems, applications of artificial immune systems in information security; association with any professional associations and intelligent networks. He is also a committee member of intelligent robots committee and natural computing committee in the Association of Artificial Intelligence of China.

Bharat Bhargava received the BE degree from the Indiana Institute of Science and the MS and PhD degrees in EE from Purdue University. He is a professor of computer sciences at Purdue University. His research involves host authentication and key management, secure routing and dealing with malicious hosts, adaptability to attacks, and experimental studies. Related research is in formalizing evidence, trust, and fraud. Professor Bhargava is a fellow of the IEEE and of the Institute of Electronics and Telecommunication Engineers. He has been awarded the charter Gold Core Member distinction by the IEEE Computer Society for his distinguished service. In 1999, he received an IEEE Technical Achievement award for a major impact of his decade long contributions to foundations of adaptability in communication and distributed systems.

Norman O. Ahmed received the BS degree in Computer Science from the Utica College of Syracuse University in 2002 and the MS degree in Computer Science from the Syracuse University in 2006. Since 2009, he has been studying for PhD degree in the Department of Computer Science, Purdue University. He is also working at the Air Force Research Laboratory. His current research interests include end-to-end security of ad hoc network and security in mobile computing.