Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Network and Computer Applications ▮ (▮▮▮▮) ▮▮▮–▮▮▮
ELSEVIER
Journal of NETWORK and COMPUTER APPLICATIONS
www.elsevier.com/locate/jnca

Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach

Lijun Qian[a,*], Ning Song[a], Xiangfang Li[b]

[a]*Department of Electrical Engineering, Prairie View A&M University, Prairie View, Texas 77446, USA*
[b]*WINLAB, Rutgers University, Piscataway, NJ 08854, USA*

Received 27 July 2005; accepted 28 July 2005

Abstract

Various routing attacks for single-path routing have been identified for wireless ad hoc networks and the corresponding counter measures have been proposed in the literature. However, the effects of routing attacks on multi-path routing have not been addressed. In this paper, the performance of multi-path routing under wormhole attack is studied in detail. The results show that multi-path routing is vulnerable to wormhole attacks. A simple scheme based on statistical analysis of multi-path (called SAM) is proposed to detect such attacks and to identify malicious nodes. Comparing to the previous approaches (for example, using packet leash), no special requirements (such as time synchronization or GPS) are needed in the proposed scheme. Simulation results demonstrate that SAM successfully detects wormhole attacks and locates the malicious nodes in networks with different topologies and with different node transmission range. Moreover, SAM may act as a module in local detection agents in an intrusion detection system (IDS) for wireless ad hoc networks.

Keywords: Wormhole attack; Multi-path routing; Wireless ad hoc network

*Corresponding author. Tel.: +19368579918; fax: +19368574780.
E-mail addresses: liqian@pvamu.edu (L. Qian), NSong@pvamu.edu (N. Song), xfli@winlab.rutgers.edu (X. Li).

1084-8045/$ - see front matter © 2005 Published by Elsevier Ltd.
doi:10.1016/j.jnca.2005.07.003

1. Introduction

The application of multi-path techniques in wireless ad hoc networks attracts a lot of attention recently because multi-path routing (MR) reduces the damages of unreliable wireless links and the constantly changing network topology. Pham and Perreau (2003) show that multi-path routing provides better performance in congestion and capacity than single-path routing. When single-path on-demand routing protocol such as AODV (Perkins et al., 2003) is used in highly dynamic wireless ad hoc networks, a new route discovery is needed in response to every route break. Each route discovery is associated with high overhead and latency. This inefficiency can be avoided by having multiple paths available and a new route discovery is needed only when all paths break.

In view of the advantages of multi-path routing in multi-hop wireless ad hoc networks, recently there are several works on modeling, analyzing and developing reliable and efficient data delivery techniques using multiple paths, for example, Tsirigos and Haas (2004a, b), Vasudevan and Sanyal (2004). However, all of them focus on studying data delivery techniques with diversity coding (Ayanoglu et al., 1993) using multiple paths rather than the security aspects of multi-path routing itself.

Various routing attacks have been identified and specific solutions to each type of the attacks are provided in the literature for single-path routing. Examples include the wormhole attack (Hu et al., 2003a), rushing attack (Hu et al., 2003b), and blackhole attack (Patcha and Mishra, 2003). Although there are many studies on single-path routing security, very little is known about multi-path routing security. For example, it is not clear how multi-path routing will perform under various routing attacks. Security enhancement of single-path routing protocols have also been proposed recently, for example, SEAD (Hu et al., 2002a), SRP (Papadimitratos and Haas, 2002), Ariadne (Hu et al., 2002b), ARAN (Sanzgiri et al., 2002), and secure AODV (Zapata, 2002). However, the appropriate security enhancement mechanism for multi-path routing is not yet studied. It is pointed out later in this section using wormhole attack as an example that although some of the wormhole detection schemes for single-path routing may be extended to multi-path routing, there is an alternative and better way to detect wormhole by taking advantage of the resulted routes from multi-path routing, thus reduce overhead and increase efficiency.

1.1. Multi-path routing

Split multi-path routing (SMR), introduced by Lee and Gerla (2001), is an on-demand routing protocol that constructs maximally disjoint paths. When the source needs a route to the destination but no route information is known, it floods the ROUTE REQUEST (RREQ) message to the entire network. Because the packet is flooded, several duplicates that traversed through different routes reach the destination. The destination node selects multiple disjoint routes and sends ROUTE REPLY (RREP) packets back to the source via the chosen routes. SMR is based on

DSR but using a different packet forwarding mechanism. While DSR discards duplicate RREQ, SMR allows intermediate nodes to forward certain duplicate RREQ in order to find more disjoint paths. In SMR, intermediate nodes forward the duplicate RREQ that traversed through a different incoming link than the link from which the first RREQ is received, and whose hop count is not larger than that of the first received RREQ. For example, in Fig. 1, if node "f" broadcasts a RREQ to destination node "j", the intermediate node "c" will receive many duplicate RREQs. Suppose that the first RREQ arrived at "c" is from "f → a → b → c", whose hop counter is 3, then any RREQ whose hop counter is larger than 3 will be discarded. In addition, any RREQ comes from node "b" will also be dropped, such as the one from "f → g → b → c". In this example, only RREQ from "f → g → h → c" will be forwarded besides the first received RREQ.

In this paper, an on-demand multi-path routing protocol similar to SMR is used for route discovery. When a source needs a new route, it floods a RREQ to the entire network and waits for responses. The intermediate node will forward the first received RREQ and the duplicate RREQ that has not been forwarded by the node and whose hop count is not larger than that of the first received RREQ. The destination will wait certain amount of time (a design parameter) after receiving the first RREQ to collect all the obtained routes. The difference of the multi-path routing protocol used in this paper from SMR in Lee and Gerla (2001) is that the intermediate nodes do not consider the incoming link of the duplicate RREQ, thus it may find more routes than SMR. In the example above, unlike the case in SMR, node "c" will forward the RREQ from "f → g → b → c" as well.

1.2. Wormhole attack

Wormhole attack (Hu et al., 2003a; Wang et al., preprint; Wang and Bhargava, 2004; Zhen and Srinivas, 2003; Hu and Evans, 2004) is caused by attacker who tunnels packets at one point to another point in the network, and then replays them into the network from that point. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols. Since the tunneled distances are longer than the normal wireless transmission range of a single hop, the source will prefer the path including the attackers. Then the attackers may perform various attacks, such as the black hole attacks (by dropping all data packets) and grey hole attacks (by selectively dropping data packets) (Patcha and Mishra, 2003).

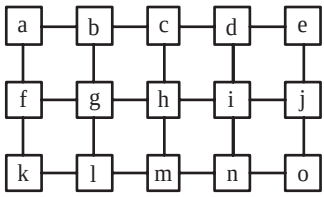

Fig. 1. A multi-path routing example.

Wormhole attacks may be categorized as open, half-open and closed, as described in Wang et al. (preprint). An example is given in Fig. 2. In (a), the wormhole nodes "b" and "c" tunnel the RREQ without appending any information to it. Then it looks like "a" and "d" are directly connected without any other nodes exist in between. This is the "open wormhole". In (b), the wormhole node "b" appends its information. The link looks like "a → b → d", with one wormhole node included. This is called a "half-open wormhole". In (c), the wormhole nodes "b" and "c" both append their information. Then the link becomes "a → b → c → d", with both wormhole nodes exist in the route. This is named "closed wormhole".

Because the wormhole nodes do not modify or fabricate packet, cryptographic techniques can not detect this type of attack. It is a severe attack in ad hoc networks that is particularly challenging to defend against.

In Hu et al. (2003a), "packet leash" is introduced to defend against wormhole attack by adding information about geography or time to a packet to restrict the packet's maximum allowed transmission distance. This scheme requires time synchronization and GPS.

Secure tracking of node encounters (SECTOR) is proposed in Capkun et al. (2003) that applied similar principle as packet leashes, with the difference that it measures the distance at a single hop. SECTOR requires special hardware at each node to respond to a one-bit challenge with one-bit response immediately using MAD protocol (Capkun et al., 2003).

Another approach is proposed recently by Wang et al. (preprint). The basic idea is to use an end-to-end mechanism where each node will append its time and location information to a detection request, and the destination will perform checks on the

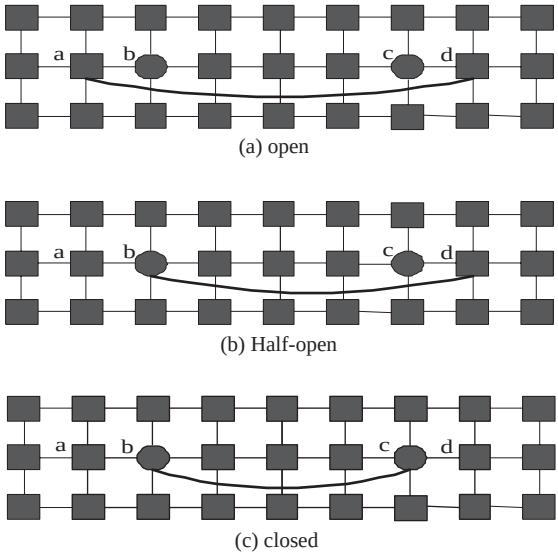

Fig. 2. 3 types of wormholes.

claimed time and locations to identify wormhole attacks. To lower the overhead, Cell-based Open Tunnel Avoidance (COTA) is proposed for distributed processing.

The idea of using round-trip time (RTT) to verify whether a node is a real neighbor or not is proposed by Zhen and Srinivas (2003). When a node receives a RREQ, it will check the RTT. If the RTT exceeds a threshold, the RREQ will be dropped. Otherwise, the RREQ is a legal request. This mechanism can detect replay attacks and sort out wormhole attacks in AODV. However, it implies that the routing messages cannot be altered and all nodes are time synchronized, and a key pair exists between any node pair.

Multi-dimensional scaling (MDS) is adopted in Wang and Bhargava (2004) to detect wormholes in sensor networks. The approach is based on the observation that the network with normal nodes has different visualization from that with attack nodes. It requires that the distance for almost all node pairs can be obtained by a center node (with more power and capacity). Then the layout of the network can be reconstructed and visualized.

A cooperative protocol whereby nodes share directional information is proposed in Hu and Evans (2004) to prevent wormhole attacks assuming that nodes are equipped with directional antennas. It adopts directional antennas technique to maintain accurate information about their neighbors. Directional antennas can transmit farer in some sector than in other sectors, so they can obtain relative direction information. When cooperating with other nodes, possible neighbors can be verified.

The performance of multi-path routing under routing attacks will be investigated in this paper. Specifically, the performance of an on-demand multi-path routing protocol (similar to SMR proposed in Lee and Gerla (2001)) under wormhole attack (Hu et al., 2003a), is our principle interest here and is used as an example in a series of simulation studies. The objectives of this paper are: (1) to examine the performance of multi-path routing under wormhole attacks, (2) to propose a statistical analysis scheme to detect routing attacks (specifically wormhole attacks) and to identify malicious nodes, based solely on the information collected by multi-path routing, and (3) to extend the statistical analysis approach to other source routing schemes (not necessarily multi-path routing) as long as enough routing information is available.

Although some of the proposed wormhole detection schemes (such as packet leash Hu et al., 2003a) may be extended to multi-path routing, the computational complexity and the associated overhead will increase dramatically because the number of paths involved in a multi-path routing is usually an order of magnitude higher than that in a single-path routing. In addition, some of the schemes may need to be modified significantly for multi-path routing. For example, in a multi-path routing, a node may report different location and/or time information for the same routing request which would be considered an anomaly in single-path routing schemes. More importantly, note that all the schemes for detection and prevention of routing attacks and security enhancement in single-path routing need to change routing protocols and/or add additional security services or systems in the network. On the contrary, the proposed scheme, called statistical analysis of multi-path

(SAM), does not need to change routing protocols. In addition, it requires very little security services or test systems. SAM applies statistical analysis to the collected routes, thus it only introduces very limited overhead. SAM can be a stand-alone module or be incorporated into an intrusion detection system.

The rest of the paper begins with performance analysis of multi-path routing under wormhole attacks in Section 2. Because the results show that multi-path routing is vulnerable to wormhole attack, a statistical analysis approach (SAM) is proposed in Section 3 and extensive simulations are carried out to evaluate the effectiveness of the proposed scheme. The role of SAM in an intrusion detection system is also highlighted. This is followed by the discussion in Section 4 of the advantages and drawbacks of SAM, and its potential applicability under various routing attacks and using different routing protocols. Conclusion and future work are given in Section 5.

2. Multi-path routing under wormhole attack

In this section, the performance of an on-demand multi-path routing protocol (MR) under wormhole attack will be compared side-by-side with DSR using the same simulation setup. The percentage of obtained routes affected by wormhole attack will be used as the performance criterion.

2.1. Simulation setup

The performance of MR and DSR under wormhole attack is evaluated through simulations. Two types of network topology are considered: cluster topology (Fig. 3) and uniform topology (Fig. 4). In both topologies, legitimate nodes are denoted by dark squares and a pair of attackers are denoted by circles. And it is assumed that each node can only communicate with its immediate neighbors (1-tier system).

The cluster topology imitates typical wireless ad hoc network where sparse nodes are between two hot spots. For example, people in a library use wireless ad hoc networks to communicate with people in a nearby building. In this setup, there are 2

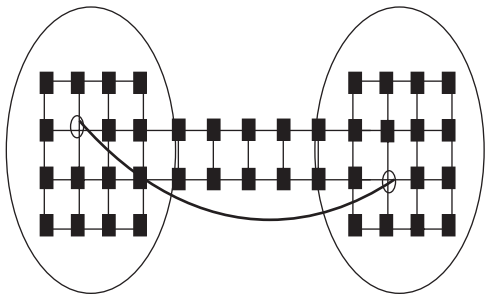

Fig. 3. Topology of 2-cluster system.

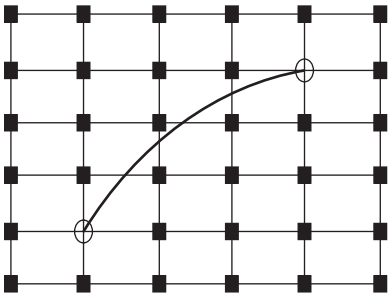

Fig. 4. Topology of uniform system.

Table 1
Percentage of routes affected by wormhole attack

Run	Cluster		Uniform	
	MR	DSR	MR	DSR
1	1.00	1.00	1.00	1.00
2	1.00	1.00	0.50	0.67
3	1.00	1.00	0.67	0.67
4	1.00	1.00	1.00	1.00
5	1.00	1.00	1.00	1.00
6	1.00	1.00	0.44	0.50
7	1.00	1.00	0.33	0.50
8	1.00	1.00	0.33	0.50
9	1.00	1.00	0.25	0.67
10	1.00	1.00	0.25	0.50
Avg.	1.00	1.00	0.58	0.70

clusters with 16 nodes (4×4) in each cluster and 10 nodes (2×5) between the 2 clusters (Fig. 3). In each run of the simulation, the source is randomly chosen in one cluster and the destination is randomly chosen in another cluster. Uniform topology is also considered, where 36 nodes (6×6) are uniformly distributed in a square area in this setup (Fig. 4). In each run of the simulation, the source is randomly chosen from left side of the network (close to one attacker) and the destination is randomly chosen from the opposite side (close to another attacker). The two attackers are assumed to be at fixed positions and they are able to tunnel RREQ between each other during all simulations. Node mobility is not considered in this simulation study.

2.2. *Observations from the simulation results*

- The percentage of routes affected by wormhole attack in 10 runs is shown in Table 1. A route is considered affected if it contains the tunneled link between the

Table 2
Overhead of route discovery

Run	Cluster		Uniform	
	MR	DSR	MR	DSR
1	1265	280	310	220
2	547	219	583	228
3	372	267	368	216
4	600	249	558	229
5	1156	305	624	203
6	1505	328	644	257
7	745	262	529	263
8	401	265	691	263
9	625	230	767	225
10	459	228	471	235
Avg.	767.5	263.3	554.5	233.9

two attackers. Routes from both MR and DSR are affected by wormhole attacks. Actually, all routes are affected for both MR and DSR in cluster topology! Although MR may perform better than DSR in uniform topology, in general the simulation results show that MR is still vulnerable to wormhole attack.

- The effect of attacks depends on locations of the source, destination and attackers, as well as network topology.
- The total number of transmissions and receptions at all nodes is collected for each run and the result is shown in Table 2. It could serve as one of the cost criteria between MR and DSR for route discovery. The overhead of MR is more than twice (on average) of that of DSR, as expected. Note that it has to be justified by the frequency of new route discovery. In single-path routing, a new route discovery is needed in response to every route break. However, in multi-path routing, a new route discovery is needed only when all paths break.

3. Statistical analysis of multi-path routing information

The previous section shows that multi-path routing is vulnerable to wormhole attacks, thus a counter measure is needed. Note that some level of time synchronization and/or awareness of location information are common requirements of all approaches exist in the literature. In this paper, an entirely different approach is proposed. The main idea of the proposed scheme SAM is based on the observation that certain statistics of the discovered routes by routing protocols will change dramatically under wormhole attacks. Hence, it is possible to examine such statistics to detect this type of routing attacks and pinpoint the attackers if *enough* routing information is available (obtained by multi-path routing).

3.1. Three step procedure of wormhole attack detection

The proposed scheme for wormhole attack detection consists of the following three steps (The block diagram is shown in Fig. 5)

(1) Perform statistical analysis of the routes obtained from one route discovery. If anomalous patterns occur, go to step 2. Otherwise, choose several paths to feedback to the source node.
(2) Test the suspicious paths by sending probe packets and wait for ACKs.
(3) If attack is confirmed, report to security authority and/or notify the source and the neighbors of the attackers in order to isolate the attackers from the network.

In step 1, exactly how many routes will be chosen is a design parameter in multi-path routing protocols. It depends on multi-path data delivery strategy and specific applications, with maximum disjoint routes preferred. In addition, which statistic or joint statistics are the most effective to identify wormhole attacks is also a design parameter. In this paper, only several statistics are chosen to demonstrate the effectiveness of the proposed scheme. However, there is a lot of design space left to consider other statistics.

We assume that the network is bi-directional; that is, if node A is able to transmit to node B, then B is able to transmit to A. We also assume that wormhole attack has strong effect on the network, which means the wormhole nodes can tunnel much

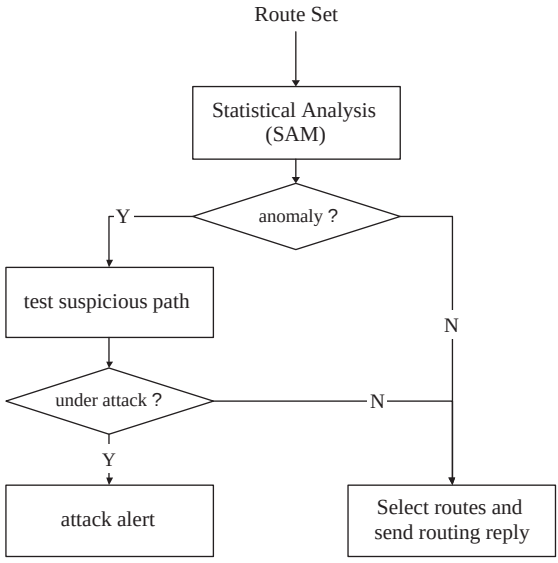

Fig. 5. Procedure of wormhole attack detection.

more than one hop. Furthermore, we do not consider other attacks such as modification and fabrication, since we only detect wormhole attack here.

The following notations are used in the proposed statistical analysis scheme:

- $\mathscr{R}$: the set of all obtained routes;
- $\mathscr{L}$: the set of all (distinctive) links in $\mathscr{R}$;
- l_i: the ith link in $\mathscr{L}$;
- n_i: the number of times that l_i appears in $\mathscr{R}$;
- n: a random variable represents the number of times that a link appears in $\mathscr{R}$;
- N: the total number of (non-distinctive) links in $\mathscr{R}$;
- p_i: the relative frequency that l_i appears in $\mathscr{R}$.

Since wormhole attack makes the tunneled link between the two attackers extremely attractive to routing requests (much less hop count than other routes), it is expected that majority of the obtained routes will contain that link. Hence, the following statistics may be examined to detect wormhole attack.

(1) The relative frequency of each (distinctive) link appears in $\mathscr{R}$ from one route discovery

$$p_i = \frac{n_i}{N}, \quad \forall l_i, \tag{1}$$

where

$$N = \sum_i n_i \tag{2}$$

and the maximum relative frequency is

$$p^{\max} = \max_i p_i. \tag{3}$$

(2) The difference between the most frequently appeared link and the second most frequently appeared link in $\mathscr{R}$ from one route discovery

$$n^{\max} = \max_i n_i, \tag{4}$$

$$i^{\max} = \arg\max_i (n_i), \tag{5}$$

$$n^{2nd} = \max_{i \neq i^{\max}} n_i, \tag{6}$$

$$\phi = \frac{n^{\max} - n^{2nd}}{n^{\max}}. \tag{7}$$

It is expected that both statistics $p^{\max}$ and ϕ will be much higher under wormhole attack than that in normal system. Together, they will help to determine whether the routing protocol is under wormhole attack. The malicious nodes can be located by the attack link which has the highest relative frequency. Note that rigorous tests may be needed to confirm a wormhole attack, as described later.

An alternative statistic is the probability mass function (PMF) of random variable n/N, the relative frequency of distinctive links in $\mathscr{R}$. The samples (n_i/N) collected from the network under normal condition will form the training set. The distribution of n/N under normal condition may be obtained by approximation using the training set and act as a profile. Then the distribution of n/N obtained using real-time samples will be compared with the profile to help determine whether the routing protocol is under wormhole attack. This approach will also provide a way to estimate the probability of high usage link using theoretical analysis since the PMF is available.

It worth pointing out that although wormhole attack is used as an example throughout this paper, the statistical analysis method proposed here may be applied to detect other routing attacks as long as certain statistics of the obtained routes change significantly under the attack. This is the first attempt to use a few statistical measure to identify routing attacks, and it is expected that more statistics need to be explored to help identify routing attacks in a complicated scenario, for example, under multiple wormhole attacks (please also refer to the discussions on multiple wormhole attacks in Section 3.4).

The test in step 2 may confirm whether the suspicious path is indeed due to a wormhole attack. Note that using probe packets to verify a wormhole attack is not a trivial problem. The schemes using location information (for example, packet leash proposed in Hu et al. (2003a), or the end-to-end approach in Wang et al. (preprint)) or packet round trip time (RTT) (Zhen and Srinivas, 2003) may be used when the nodes are time synchronized and the location information is available. These schemes *alone* have to be performed periodically to monitor the network for possible wormhole attacks. On the contrary, the verification in SAM is only needed when a wormhole attack is suspected by statistical analysis (step 1), thus it will not be performed as often.

In this paper, we suggest a different approach for step 2. In addition to wormhole detection, it may help to detect another type of denial-of-service (DoS) attack where the attacker refuses to forward data packets but behaves normally during routing.

The proposed scheme contains the following steps:

(1) The destination will send a small amount of probe packets together with some dummy data packets to the source using the route that contains the suspected wormhole.
(2) The source will identify the probe packets and send ACKs through the same routes when probe packets are received.
(3) The destination will verify a wormhole attack with high probability of confidence based on the percentage of received ACKs.

The proposed approach is to verify a wormhole attack indirectly using probe packets when location information and time synchronization are not available. The probe packets have to be constructed such that they are not distinguishable from the normal data packets by any intermediate nodes. An example probe packet format is shown in Fig. 6. We can add an encrypted (using the key shared by the source and

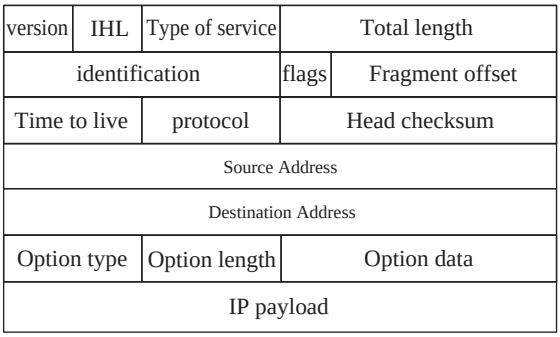

Fig. 6. Format of a probe packet.

the destination) non-decreasing sequence number in the option field of the IP header. For the option type, the copied flag is "1", which means it should be copied on fragmentation; the option class is "10", which means it is for debugging and measurement; the option number is "1". The option length is the length of sequence number and the option data is the sequence number. Since it is assumed that there exists a security association between the source and the destination, the source will be able to identify probe packets by decrypt the sequence number and send ACKs when probe packets are received. Then the destination is able to verify a wormhole attack with high probability of confidence based on the percentage of received ACKs because wormhole nodes will usually try to disrupt data flows (by performing some kind of DoS attacks, e.g. black hole or gray hole) and the statistical analysis (step 1 of SAM) already suggests that there may be wormholes.

In step 3, the malicious nodes can be identified by the attack link which has the highest relative frequency. Step 3 is an important step and may form as part of the signaling messages between local detection and global coordinated detection in an intrusion detection system (IDS).

In case that there is a bottleneck link in the network, a topology discovery (Deb et al., 2004) may be carried out to check whether the suspected link is only a bottleneck link or not. However, this checking only needs to be done in a much longer time scale. Note that bottleneck link seldomly exists in a dense network or network with high node mobility.

3.2. SAM in IDS

The typical anomaly IDS should be both distributed and cooperative to satisfy the needs of mobile wireless ad hoc networks (Zhang et al., 2003). Each node will act as an agent of IDS to detect the attack locally and independently; on the other hand, it will collaborate with other nodes in the network, so as to identify and notify attack behaviors. In the system aspect, each agent (node) will implement a serial process. It firstly collects data locally, for example, discovered routes, movement, communication and system operation. With these data, it will then detect and evaluate anomaly

behaviors locally by implementing feature selection and classification. After obtaining the result, it will implement local response and warn the network or cooperate with other nodes to detect and locate the attacks.

SAM may act as a module of IDS, incorporating with other processes. In Fig. 7, SAM collects data when requesting multipath routing, and calculates the features, then notify the local detection module. The local detection will process by analyzing all the data from SAM and other data collection modules. The response module will implement the alarm and collaboration operations.

When a node needs to communicate with other nodes, it will generate a multipath routing request. Based on the responses, SAM module will count the links and hop count, then calculate the statistics, for example, ϕ and $p^{\max}$. Then SAM module will transfer these statistical features to the local detection module with some additional information, and wait for response. If the routing result is good, SAM will perform normal operations; if the result is suspicious, SAM could test the routes by sending packets and waiting for "ACKs" (as discussed in the previous section); otherwise, if the result shows that the discovered routes were compromised, SAM will try to locate the attackers using the link statistics. Fig. 7 shows the response model of IDS with SAM. Since the nominal values of these statistical features are relative to topology, transmission range and routing algorithm, the system will initially be trained in normal conditions with specific network topology, transmission range and routing algorithm employed in the system.

The two statistical features, ϕ and $p^{\max}$, will be processed by a sub-module in the local detection module in the IDS. Under normal trainings, it will analyze the variation of the statistical features and save the datasets. In practical tests, it processes both saved data and new data. After finishing the process, it will notify the conclusions to both the SAM module and response module so as to guide their behaviors. The conclusions are soft decisions (λ) valued by the probability of being attacked. λ is a continuous variable between 0 and 1, where 0 means being attacked with absolute certainty and 1 means no attack has been detected with absolute certainty. The module is also responsible for dynamically updating these datasets

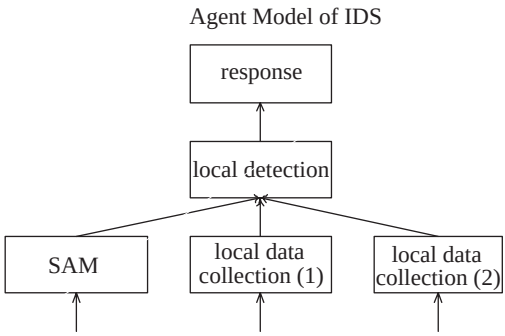

Fig. 7. Agent model of IDS with SAM.

based on the new results using the following low-pass filter with forgetting factor $0<\beta<1$ (a design parameter)

$$\phi_{new} = \lambda\beta\phi_{new} + (1-\lambda\beta)\phi_{old}, \tag{8}$$

$$p_{new}^{\max} = \lambda\beta p_{new}^{\max} + (1-\lambda\beta)p_{old}^{\max}. \tag{9}$$

Response module makes decision based on the conclusions receiving from local detection module. Then it will decide how to locate the attackers and defend other nodes from the attack or to request collaboration with other nodes in the network. Response module rely on many techniques, such as secure communication, decision algorithm and cooperative protocols, which are out of the scope of this paper.

3.3. Performance results of SAM

The performance of SAM is tested through simulations using the same setup as in Section 2.1. The proposed statistics for normal system and attacked system are compared under different network topologies and different node transmission range.

A sample PMF of n/N, the relative frequency of distinctive links in $\mathscr{R}$, is plotted in Fig. 8 using results from a single run of network with 1-tier cluster topology. The further right side of the figure the data locates, the higher frequency the represented link appears in $\mathscr{R}$. In this test, the highest relative frequency is 9% in normal system, whereas in attacked system, the highest relative frequency is more than 15%. Furthermore, the link with the highest relative frequency locates far apart from other

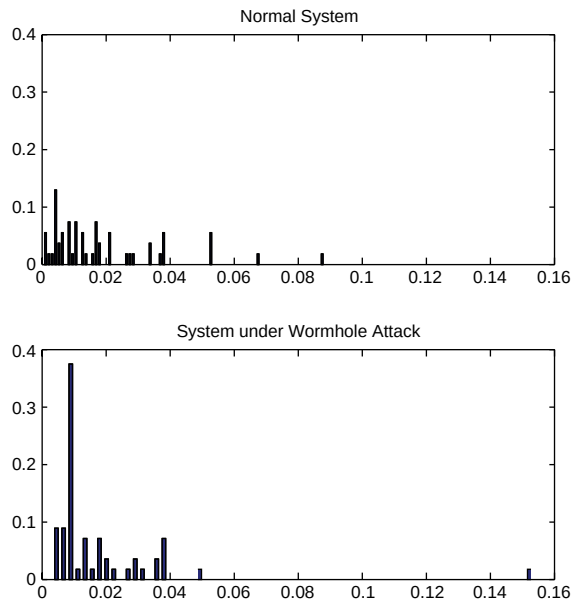

Fig. 8. PMF of n in normal condition and under wormhole attack.

links in attacked system, which corresponds to the fact that the attack link appears many more times in the obtained routes than other links.

(1) *Effect of network topology*: The effect of network topology is tested in 10 runs using cluster and uniform topologies and the results are shown in Figs. 9 and 10 in

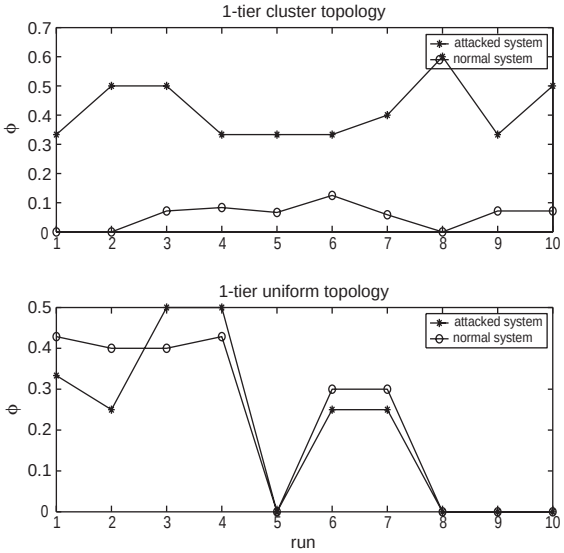

Fig. 9. ϕ of 1-tier network using MR.

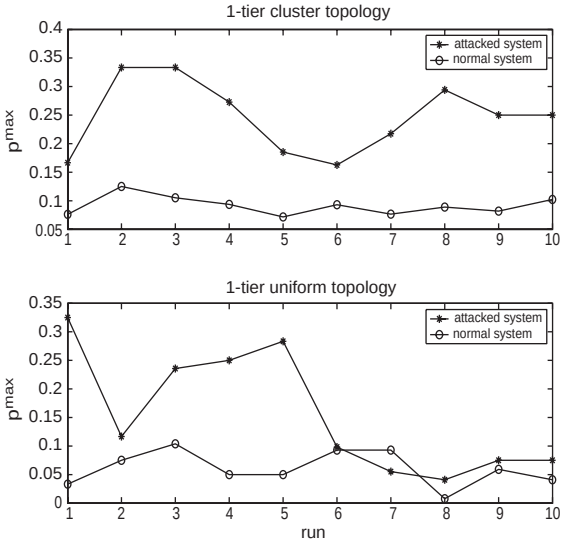

Fig. 10. $p^{\max}$ of 1-tier network using MR.

terms of ϕ and $p^{\max}$. Both ϕ and $p^{\max}$ are larger in attacked system than that in normal system with cluster topology. However, this is not the case for system with uniform topology. This is because the attack link in uniform topology is so short (6-hop) that it has much less effect on route discovery than the long attack link (10-hop) in cluster topology. Hence, the simulation is repeated for a network with uniform topology with 6×10 nodes and the length of the attack link increases to 10-hop. The results are plotted in Fig. 11, which shows that both ϕ and $p^{\max}$ are larger in attacked system than that in normal system with unfirm topology as well. In several simulation runs (number 1,7 and 10), $\phi = 0$ in attacked system indicates that there are at least two links which have the same highest relative frequency. This special case happens when the attackers locate at the same row or column of the source node or destination node. The above simulations demonstrate that the length of the tunneled link between attackers has to be long enough to launch a wormhole attack, and ϕ and $p^{\max}$ can be used *together* to successfully detect it in networks with cluster or uniform topologies.

The effect of network topology is further tested in 10 runs of a network with random topology using MR. The (X,Y) coordinates of the nodes are randomly generated in a square area, as shown in Fig. 12. The simulation results shown in Fig. 13 indicate that $p^{\max}$ can be used to successfully detect a wormhole attack in networks with random topologies.

(2) *Effect of node transmission range*: In a wireless ad hoc network, the transmission range of nodes plays an important role in determining network topology. In a 1-tier system, each node can only communicate with its immediate neighbors (nodes one hop away). Similarly, in a k-tier system, each node can communicate with its neighbors up to k hops away.

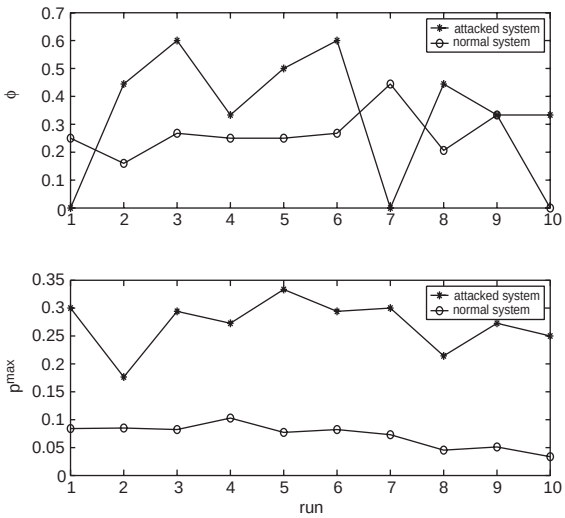

Fig. 11. ϕ and $p^{\max}$ of 1-tier network with 6×10 uniform topology.

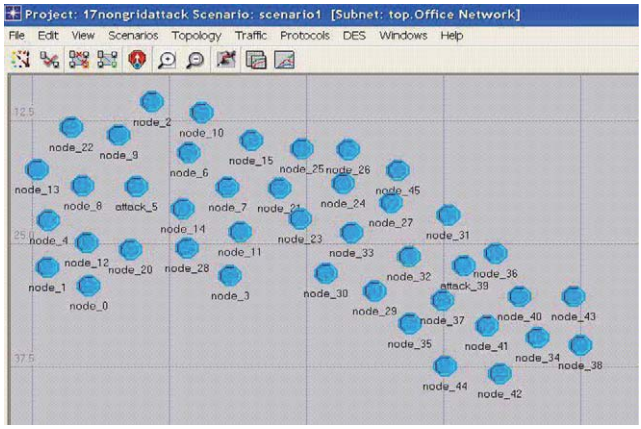

Fig. 12. A network with random topology using MR.

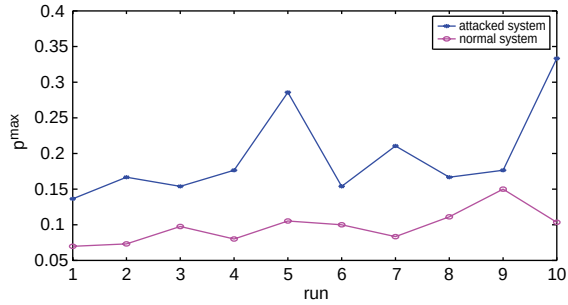

Fig. 13. $p^{\max}$ of a network with random topology using MR.

It is demonstrated in Figs. 14 and 15 that both ϕ and $p^{\max}$ are larger in attacked system than that in normal system in both 1-tier and 2-tier systems with cluster topology. As long as the length of the attack link is much longer than the node transmission range, wormhole attack will be effective and the feature of ϕ and $p^{\max}$ will enable SAM to detect the attack when it is most needed.

(3) *Effect of routing algorithm*: In this part of the simulation, ϕ and $p^{\max}$ are calculated from the routes obtained by MR and DSR, respectively. The feature of $p^{\max}$ remains the same but not ϕ (Figs. 16, 17). The results indicate that it is possible to perform statistical analysis to detect wormhole attacks using the routes obtained from routing protocols other than MR.

3.4. Multiple wormhole attacks

The performance of the proposed scheme under multiple wormhole attacks is evaluated in 10 runs of a network under two wormhole attacks. The results are

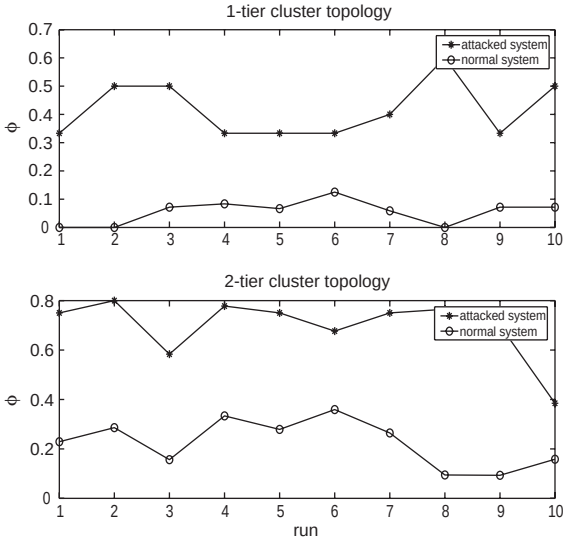

Fig. 14. ϕ of cluster systems with different transmission range for MR.

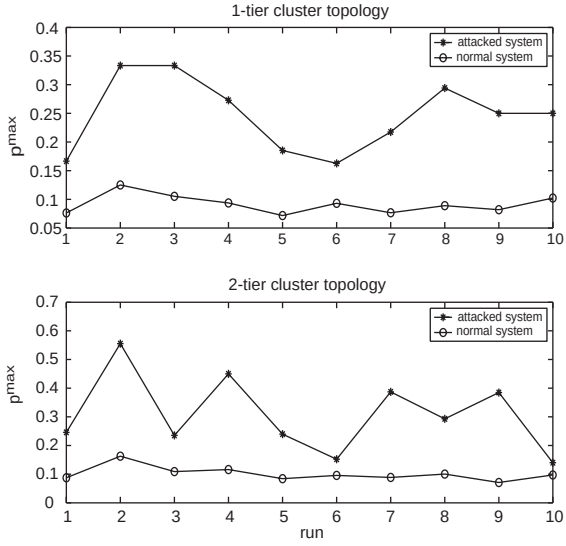

Fig. 15. $p^{\max}$ of cluster systems with different transmission range for MR.

summarized in Fig. 18. $p^{\max}$ is much higher in both attacked networks than that in the normal networks. It seems that the variance of $p^{\max}$ becomes bigger as the number of wormholes increases.

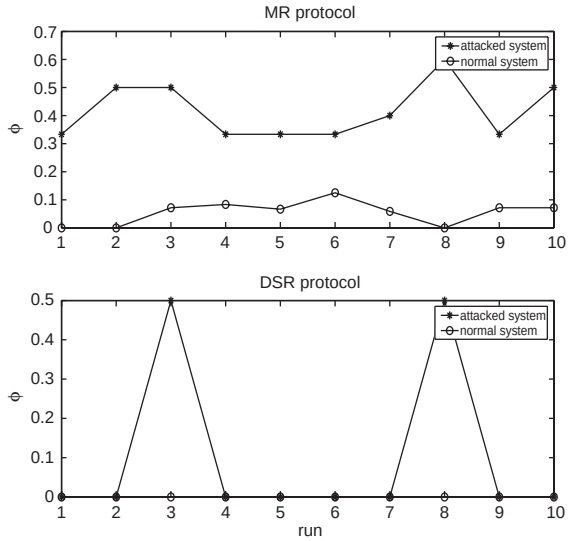

Fig. 16. ϕ of 1-tier cluster systems with different routing protocols.

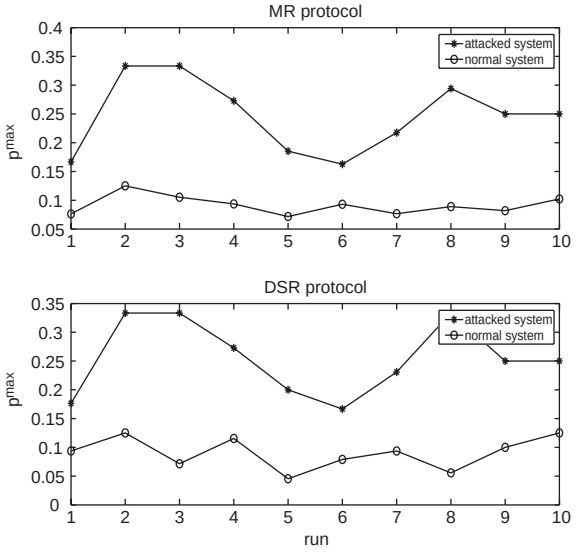

Fig. 17. $p^{\max}$ of 1-tier cluster systems with different routing protocols.

4. Discussions

The simulation results in previous section demonstrate that SAM is effective in detecting wormhole attacks when enough routes are available. In addition, SAM has the following advantages:

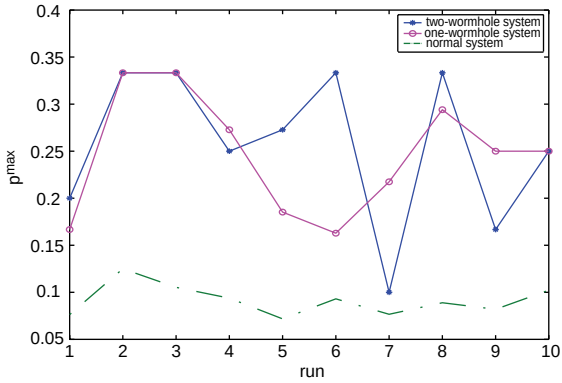

Fig. 18. $p^{\max}$ of a network under no/one/two wormhole attacks.

- SAM introduce very limited overhead. It only needs the route information collected by route discovery, which has to be done anyway in any source routing. Only the destination node need to run SAM. Other overhead introduced by probe packets is also limited because the checking in step 2 of SAM is only performed after the suspected link is identified (which should not happen often).
- SAM works well under different network topologies and node transmission range. If the node transmission range grows large enough that comparable to the tunneled link between the two attackers, then wormhole attack is no longer effective.

SAM aims at detecting wormhole attacks and may be extended to detect other routing attacks if certain statistics of the obtained routes change significantly under the attack. If a malicious node behaves normally during routing, SAM can not detect it.

In the security architectures and intrusion detection systems (IDS) proposed in Zhang et al. (2003) and Mishra et al. (2004), an IDS agent runs at each node and performs local data collection and local detection. SAM may act as a module in the local detection engine and expand the functions of the engine by examining obtained routes from multi-path routing.

Throughout this paper, the nodes are assumed to have low mobility comparing to the routing period. Indeed, if the nodes are highly mobile, the routes may become invalid soon after the routing is done. A hot-potato type of data forwarding is preferred in such scenario, as suggested in Grossglauser and Tse (2001).

Caching strategy (Hu and Johnson, 2000) has been included in most of the on-demand routing protocols proposed for wireless ad hoc networks (e.g., in DSR (Johnson et al., 2003) and AODV (Perkins et al., 2003)) to reduce the excessive route discovery delay. However, another type of attack, blackhole attack (Patcha and Mishra, 2003), may be launched where attackers do not follow the protocol and reply early without cache lookup. In the MR used in this paper, intermediate nodes

are not allowed to send RREP to the source. Thus it provides certain level of resistance to blackhole attack as well.

In addition to SMR, there are other multi-path routing protocols for wireless ad hoc networks such as Multi-path DSR (MDSR) in Nasipuri and Das (1999) and ad hoc on-demand multi-path distance vector (AOMDV) in Marina and Das (2001). Both SMR and AOMDV provide more candidate routes during route discovery than their single-path routing protocols counterpart DSR and AODV (Perkins et al., 2003), but MDSR does not. As a result, SMR and AOMDV may provide more routes for statistical analysis than MDSR.

5. Conclusion and future work

There have been many research efforts to overcome routing attacks in wireless ad hoc networks by adding security architecture, systems or services such as authentication, encryption, etc. A noteworthy feature of the proposed scheme (SAM) for detecting and locating wormhole attacks is that no security architecture, systems or services is used. Statistical analysis is the tool to detect routing anomaly as long as sufficient information of routes is available from multi-path routing. Simulation results show that SAM is successful at detecting wormhole attacks and locating the malicious nodes.

Since SAM need the node lists of each of the routes collected during route discovery to perform statistical analysis, it applies to source routing where the entire node list of the route is made available to the destination. It can not directly apply to table driven based routing algorithms, such as AODV (Perkins et al., 2003) and AOMDV in Marina and Das (2001). Modification of the proposed scheme when AODV or AOMDV is used as the routing protocol is underway.

Acknowledgements

The authors would like to thank OPNET Technologies, Inc. for providing the OPNET software to perform the simulations in this study. This research work is supported in part by the U.S. Army Research Laboratory under Cooperative Agreement No. W911NF-04-2-0054. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the US Government.

References

Ayanoglu E, I C, Gitlin R, Mazo J. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Trans Commun 1993;41:1677–86.

Capkun S, Buttyan L, Hubaux J. SECTOR: secure tracking of node encounters in multi-hop wireless networks. ACM workshop on security of ad hoc and sensor networks (SASN), Washington, DC, USA; October 2003. p. 1–12.

Deb B, Bhatnagar S, Nath B. STREAM: sensor topology retrieval at multiple resolutions. Telecommun Syst 2004;26:285–320.

Grossglauser M, Tse D. Mobility increases the capacity of ad-hoc wireless networks. Proceedings of IEEE INFOCOM; April 2001. p. 1360–9.

Hu L, Evans D. Using directional antennas to prevent wormhole attacks. Network and distributed system security symposium (NDSS), San Diego; February 2004.

Hu Y, Johnson D. Caching strategies in on-demand routing protocols for wireless ad hoc networks. Proceedings of MobiCom; August 2000. p. 231–42.

Hu Y, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the 4th IEEE workshop on mobile computing systems & applications (WMCSA 2002), IEEE, Calicoon, NY; June 2002a. p. 3–13.

Hu Y, Perrig A, Johnson DB. Ariadne: a secure on-demand routing protocol for ad hoc networks. MobiCom 2002, Atlanta, GA; September 2002b. p. 12–23.

Hu Y-C, Perrig A, Johnson DB. Packet leashes: a defense against wormhole attacks in wireless ad hoc networks. Proceedings of INFOCOM 2003; April 2003a. p. 1976–86.

Hu Y-C, Perrig A, Johnson DB. Rushing attacks and defense in wireless ad hoc network routing protocols. ACM workshop on wireless security (WiSe 2003), Westin Horton Plaza Hotel, San Diego, CA; September 2003b. p. 30–40.

Johnson D, Maltz D, Hu Y. The dynamic source routing protocol for mobile ad hoc networks. Internet draft, draft-ietf-manet-dsr-09.txt, April 2003.

Lee S, Gerla M. Split multipath routing with maximally disjoint paths in ad hoc networks. Proceedings of IEEE ICC, vol. 10; May 2001. p. 3201–5.

Marina MK, Das SR. Ad hoc on-demand multipath distance vector routing protocol. Proceedings of IEEE ICNP; November 2001.

Mishra A, Nadkarni K, Patcha A. Intrusion detection in wireless ad hoc networks. IEEE Wireless Commun 2004;11(1):48–60.

Nasipuri A, Das SR. On-demand multipath routing for mobile ad hoc networks. Proceedings of the 8th international conference on computer communications and networks (IC3N), Boston, MA; 1999.

Papadimitratos P, Haas ZJ. Secure routing for mobile ad hoc networks. SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002), San Antonio, TX; January 2002.

Patcha A, Mishra A. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. Proceedings of RAWCON '03; 2003. p. 75–8.

Perkins C, Belding-Royer E, Das S. Ad hoc on-demand distance vector (AODV) routing. RFC 3561; July 2003.

Pham P, Perreau S. Performance analysis of reactive shortest path and multi-path routing mechanism with load balance. Proceedings of INFOCOM 2003; 2003. p. 251–9.

Sanzgiri K, Dahill B, Levine B, Shields C, Belding-Royer E. A secure routing protocol for ad hoc networks. Proceedings of the 10th IEEE international conference on network protocols (ICNP'02), Paris, France; November 2002. p. 78–87.

Tsirigos A, Haas ZJ. Analysis of multipath routing—part I: the effect on the packet delivery ratio. IEEE Trans Wireless Commun 2004a;3(1):138–46.

Tsirigos A, Haas ZJ. Analysis of multipath routing—part II: mitigation of the effects of frequently changing network topologies. IEEE Trans Wireless Commun 2004b;3(2):500–11.

Vasudevan R, Sanyal S. A novel multipath approach to security in mobile ad hoc networks (MANETs). Proceedings of the international conference on computers and devices for communication (CODEC'04), Kolkata, India; January 2004.

Wang W, Bhargava B. Visualization of wormholes in sensor networks. ACM Workshop on Wireless Security (WiSe 2004), Philadelphia, PA; October 2004. p. 51–60.

Wang W, Bhargava B, Lu Y, Wu X. Defending against wormhole attacks in mobile ad hoc networks. Preprint, http://www.cs.purdue.edu/homes/wangwc/papers/MC2R_sample_101104.pdf

Zapata M. Secure ad hoc on-demand distance vector routing. ACM mobile computing and communications review (MC2R), vol. 6(3); July 2002, p. 106–7.

Zhang Y, Lee W, Huang Y. Intrusion detection techniques for mobile wireless networks. Wireless Networks 2003;9(5):545–56.

Zhen J, Srinivas S. Preventing replay attacks for secure routing in ad hoc networks. ADHOC-NOW 2003, Lecture Notes in Computer Science, vol. 2865; 2003. p. 140–50.

Xiangfang Li is a Ph.D. student in the Department of Electrical and Computer Engineering at Rutgers University. She received her B.S. and M.S. from Beijing University of Aeronautics and Astronautics (BUAA), both in electrical engineering. Her major research interests are in wireless communications and mobile computing, especially in radio resource management, cross-layer design and wireless network security.

Lijun Qian is an assistant professor in the Department of Electrical Engineering at Prairie View A&M University. He received his B.S. from Tsinghua University in Beijing, M.S. from Technion-Israel Institute of Technology, and Ph.D. from WINLAB, Rutgers University, all in electrical engineering. Before joining PVAMU, he was a researcher at Networks and Systems Research Department of Bell Labs in Murray Hill, NJ. His major research interests are in wireless communications and networking technologies, especially in radio resource management, protocol design, TCP/RLP optimization and network security.

Ning Song is a Ph.D. student in the Department of Electrical Engineering at Prairie View A&M University. He received his B.S. in Electrical Engineering from Wu Han University of Technology in 1995, and M.S. in Applied Mathematics from University of Science & Technology Beijing in 1998. He worked as a programmer in China from 1998 to 2003, mainly in the fields of telecommunications and network security. His major research interests are in wireless sensor networks, wireless security protocols, and design of intrusion detection systems.