Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path

Lijun Qian and Ning Song
Department of Electrical Engineering
Prairie View A&M University
Prairie View, Texas 77446
Email: Lijun_Qian, NSong@pvamu.edu

Xiangfang Li
WINLAB
Rutgers University
Piscataway, NJ 08854
Email: xfli@winlab.rutgers.edu

***Abstract*— The application of multi-path techniques in wireless ad hoc networks is advantageous because multi-path routing provides means to combat the effect of unreliable wireless links and constantly changing network topology. In this paper, the performance of multi-path routing under wormhole attack is studied in both cluster and uniform network topologies. Because multi-path routing is vulnerable to wormhole attacks, a scheme called Statistical Analysis of Multi-path (SAM) is proposed to detect such attacks and to identify malicious nodes. As the name suggests, SAM will detect wormhole attacks and identify attackers by statistically analyzing the information collected by multi-path routing. Neither additional security services or systems nor security enhancement of routing protocols is needed in the proposed scheme. Simulation results demonstrate that SAM successfully detects wormhole attacks and locates the malicious nodes in networks with cluster and uniform topologies and with different node transmission range.**

I. Introduction

The application of multi-path techniques in wireless ad hoc networks is natural, as multi-path routing (MR) allows diminishing the effect of unreliable wireless links and the constantly changing network topology. Pham and Perreau [6] 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 [15] 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 avaialble 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, [4] [5] [7]. However, all of them focus on studying data delivery techniques with diversity coding [11] 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 [8], rushing attack [9], and blackhole attack [10]. However, it is not clear how multi-path routing will perform under these routing attacks.

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 [1]) under wormhole attack [8], 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. 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 or introduce additional security services or systems, thus it only introduces very limited overhead on statistical analysis. SAM can be a stand-alone module or incorporate into an intrusion detection system.

The rest of the paper begins with performance analysis of multi-path routing under wormhole attack 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. 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 different routing protocols. Conclusion and future work are given in Section 5.

II. 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.

Split Multi-path Routing (SMR), introduced by Lee and Gerla [1], is an on-demand routing protocol that constructs

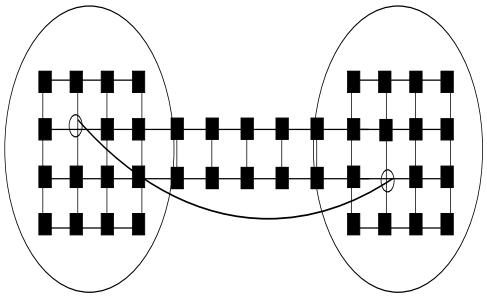

Fig. 1. Topology of 2-cluster system

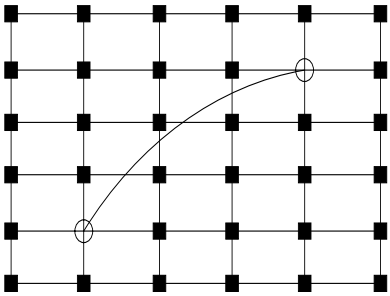

Fig. 2. Topology of uniform system

maximally disjoint paths. SMR is based on DSR but using a different packet forwarding mechanism. While DSR discards duplicate routing request (RREQ), SMR allows intermidiate 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.

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 [1] is that the intermediate nodes do not consider the incoming link of the duplicate RREQ, thus it may find more routes than SMR.

Wormhole Attack [8] is caused by attacker who tunnels packet at one point to another point in the network, and then replays them into the network from that point. It is a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols.

A. 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. 1) and uniform topology (Fig. 2). 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 clusters with 16 nodes (4×4) in each cluster and 10 nodes (2×5) between the 2 clusters (Fig. 1). 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. 2). 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 study.

	Cluster		Uniform	
Run	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

TABLE I

PERCENTAGE OF ROUTES AFFECTED BY WORMHOLE ATTACK

B. Observations from the Simulation Results

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

	Cluster		Uniform	
Run	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

TABLE II
OVERHEAD OF ROUTE DISCOVERY

III. 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. In [8], the "leash", some information about geography or time that is added to a packet to restrict the packet's maximum allowed transmission distance, is introduced to defend against wormhole attack. 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).

The following notations are used in the proposed statistical analysis scheme

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

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 $\mathcal{R}$ from one route discovery

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

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 $\mathcal{R}$ 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 determine whether the routing protocol is under wormhole attack. The malicious nodes can be identified by the attack link which has the highest relative frequency.

An alternative statistics is the probability mass function (PMF) of random variable n/N, the relative frequency of distinctive links in $\mathcal{R}$. 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 any routing attacks as long as certain statistics of the obtained routes change significantly under the attack.

A. Three Step Procedure of Wormhole Attack Detection

The proposed scheme for wormhole attack detection consists of the following three steps (also shown in Fig. 3)

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 (test) data packets and wait for ACK.
3) If attack is confirmed, report to security authority and/or notify the source and the neighbors of the attackers in order to isolate them 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 prefered.

The test in step 2 may confirm whether the suspicious path is indeed affected. In addition, it may help to detect another type

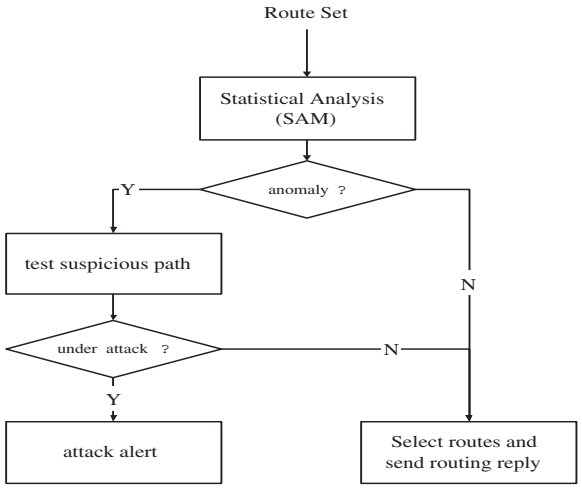

Fig. 3. Procedure of Wormhole Attack Detection

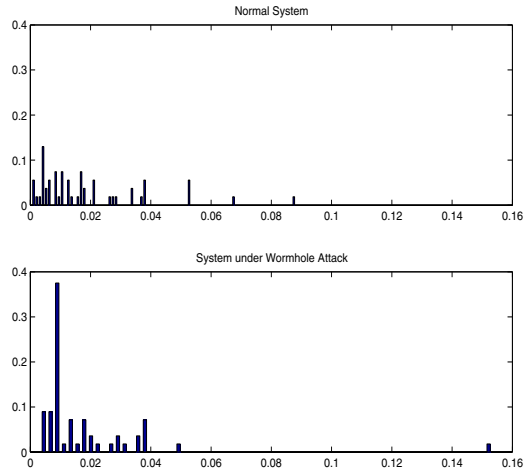

Fig. 4. PMF of n in normal condition and under wormhole attack

of Denial-of-Service (DoS) attack where the attacker refuse to forward data packets but behave normally during routing.

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).

B. Performance Results of SAM

The performance of SAM is tested through simulations using the same setup as in section II.A. 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 $\mathcal{R}$, is plotted in Fig. 4 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 $\mathcal{R}$. 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 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 Fig. 5 and 6 in 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. 7, which shows that both ϕ and p^{max} are larger in attacked system than that in normal system with unfirm

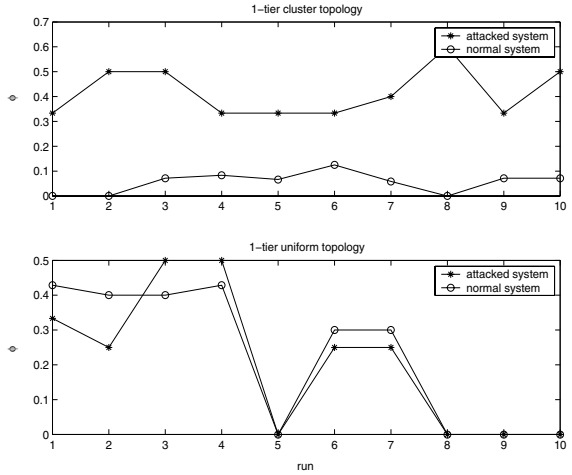

Fig. 5. ϕ of 1-tier network using MR

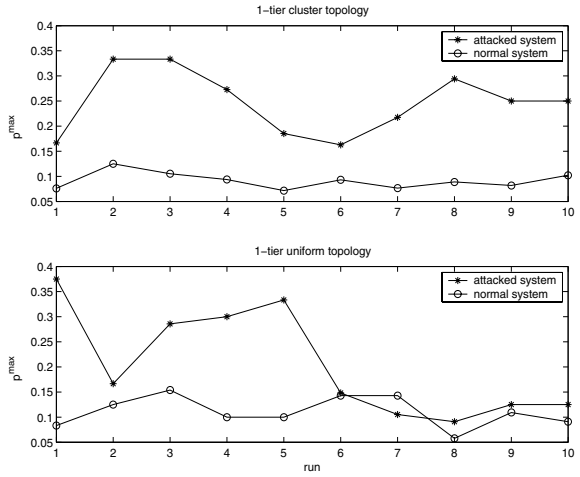

Fig. 6. p^{max} of 1-tier network using MR

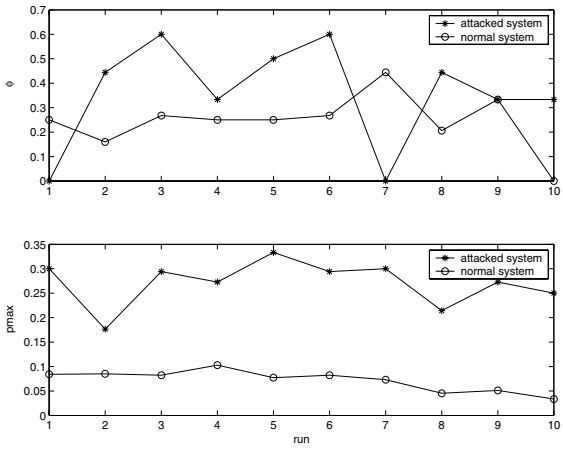

Fig. 7. ϕ and p^{max} of 1-tier network with 6×10 uniform topology

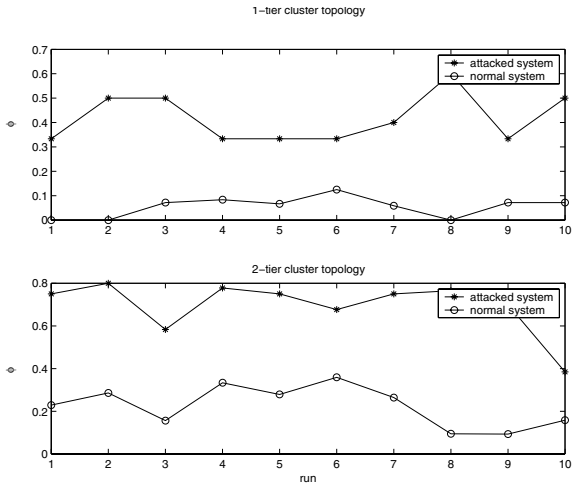

Fig. 8. ϕ of cluster systems with different transmission range for MR

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.

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.

It is demonstrated in Fig. 8 and 9 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 remain the same.

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 (Fig. 11) but not ϕ (Fig. 10). 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.

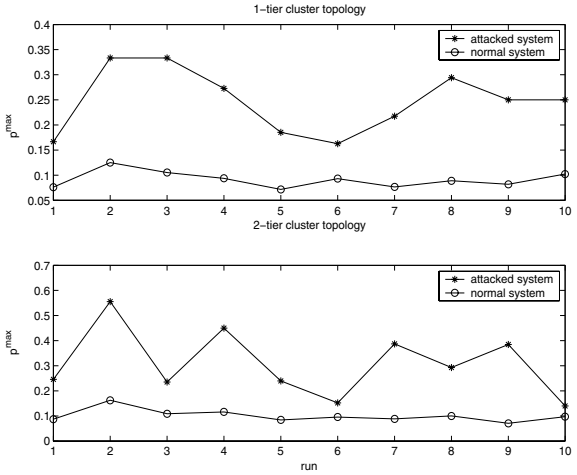

Fig. 9. p^{max} of cluster systems with different transmission range for MR

IV. 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

- SAM introduce very limited overhead. It only needs the route information collected by route discovery, which has to be done anyway in multi-path routing. Only the destination node need to run SAM.

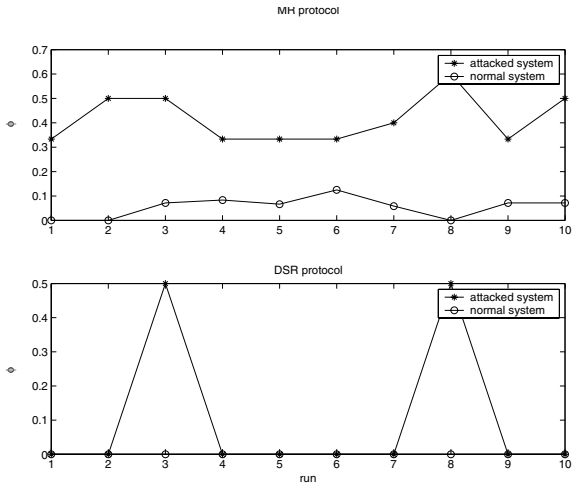

Fig. 10. ϕ of 1-tier cluster systems with different routing protocols

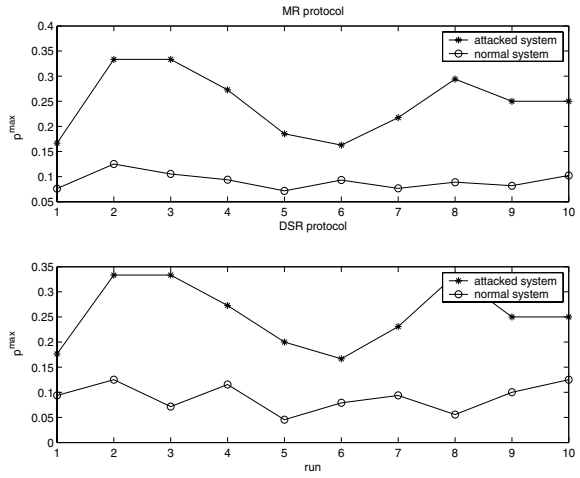

Fig. 11. p^{max} of 1-tier cluster systems with different routing protocols

- 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 [12] and [13], 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.

Caching strategy [16] has been included in most of the on-demand routing protocols proposed for wireless ad hoc networks (e.g., in DSR [14] and AODV [15]) to reduce the excessive route discovery delay. However, another type of attack, blackhole attack [10], 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.

V. 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 authetication, 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 avaialble from multi-path routing. Simulation results show that SAM is successful at detecting wormhole attacks and locating the malicious nodes.

In addition to SMR, there are other multi-path routing protocols for wireless ad hoc networks such as Multi-path DSR (MDSR) in [2] and ad hoc on-demand multi-path distance vector (AOMDV) in [3]. Both SMR and AOMDV provide more candidate routes during route discovery than their single-path routing protocols counterpart DSR and AODV [15], but MDSR does not. As a result, SMR and AOMDV may provide more routes for statiscal analysis than MDSR. Evaluation of the proposed scheme using SMR or AOMDV as the multi-path routing protocol is underway.

Acknowledgment

The authors would like to thank OPNET Technologies, Inc. for providing the OPNET software to perform the simulations in this study.

References

[1] S. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks", *Proc. of IEEE ICC*, Vol.10, pp.3201-3205, May 2001.

[2] A. Nasipuri and S.R. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Networks", *Proceedings of the 8th Int. Conf. on Computer Communications and Networks (IC3N)*, Boston, MA, 1999.

[3] M. K. Marina and S. R. Das, "Ad Hoc On-demand Multipath Distance Vector Routing Protocol", *Proceedings of IEEE ICNP*, Nov 2001.

[4] A. Tsirigos and Z.J. Haas, "Analysis of Multipath Routing - Part I: The Effect on the Packet Delivery Ratio", *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 138-146, Jan 2004.

[5] A. Tsirigos and Z.J. Haas, "Analysis of multipath routing - part II: mitigation of the effects of frequently changing network topologies", *IEEE Transactions on Wireless Communications*, vol. 3, no. 2, pp. 500-511, Mar 2004.

[6] P. Pham and S. Perreau, " Performance analysis of reactive shortest path and multi-path routing mechanism with load balance", *Proc. of INFOCOM 2003*, pp.251-259, 2003.

[7] R. Vasudevan and S. Sanyal, "A novel multipath approach to security in mobile ad hoc networks (MANETs)", *Proc. of Intl Conf. Computers and Devices for Communication (CODEC'04)*, Kolkata, India, January 2004.

[8] Y.-C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc NetworksNetworks", *Proc. of INFOCOM 2003*, pp.1976-1986, Apr 2003.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", *ACM Workshop on Wireless Security (WiSe 2003)*, pp. 30-40, Westin Horton Plaza Hotel, San Diego, CA, Sep 2003.

[10] A. Patcha and A. Mishra, "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks", *Proc. of RAWCON '03*, pp.75-78, 2003.

[11] E. Ayanoglu, C. I, R. Gitlin and J. Mazo, "Diversity Coding for Transparent self-healing and fault-tolerant Communication Networks", *IEEE Transactions on Communications*, Vol.41, pp.1677-1686, 1993.

[12] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", *Wireless Networks*, Vol. 9, No. 5, pp. 545-556, Sep 2003.

[13] A. Mishra, K. Nadkarni and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks", *IEEE Wireless Communications*, Vol. 11, No. 1, pp. 48-60, February 2004.

[14] D. Johnson, D. Maltz and Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", *Internet Draft*, draft-ietf-manet-dsr-09.txt, Apr 2003.

[15] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", *RFC 3561*, July 2003.

[16] Y. Hu and D. Johnson, "Caching Strategies in On-Demand Routing Protocols for Wireless Ad Hoc Networks", *Proceedings of MobiCom*, pp.231-242, Aug 2000.