The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (pp. 183–191)
http://www.isecure-journal.org

Short Paper

A Two-Phase Wormhole Attack Detection Scheme in MANETs

Shiva Shamaei [1,*], and Ali Movaghar [1]
[1] *Performance and Dependability Lab (PDL),Department of Computer Engineering Sharif University of Technology,Tehran,Iran*

ARTICLE INFO.

Article history:
Received: 16 December 2013
Revised: 9 November 2014
Accepted: 3 February 2015
Published Online: 13 February 2015

Keywords:
Mobile ad-hoc Networks, Wormhole Detection Scheme, Wormhole Attack, Wormhole Tunnel.

ABSTRACT

Mobile ad-hoc networks (MANETs) have no fixed infrastructure, so all network operations such as routing and packet forwarding are done by the nodes themselves. However, almost all common existing routing protocols basically focus on performance measures regardless of security issues. Since these protocols consider all nodes to be trustworthy, they are prone to serious security threats. Wormhole attack is a kind of such threats against routing processes which is particularly a challenging problem to detect and prevent in MANETs. In this paper, a two-phase detection scheme is proposed to detect and prevent wormhole attacks. First phase checks whether a wormhole tunnel exists on the selected path or not. If there is such a tunnel, the second phase is applied to confirm the existence of the wormhole attack, and locate a malicious node. The proposed detection scheme can appropriately detect all types of this kind of attacks such as in-band and out-of-band ones in different modes such as hidden or exposed, without any need of special hardware or time synchronization. In order to evaluate the performance of the proposed scheme, some various scenarios are simulated in the NS-2 simulator, and different measures are assessed. The results obtained from simulating the proposed scheme and other benchmarks indicate that in most criteria considered in this paper, the proposed scheme outperforms the proposed methods in prior works.

1 Introduction

Mobile ad-hoc networks (MANETs) - due to their characteristics such as lack of infrastructure, dynamic topology and distributed routing [1] - are more prone to security attacks as compared to wired networks. One of these security attacks is the wormhole attack which is enumerated as one of the most threatening and dangerous attacks in MANETs [2, 3].

Wormhole attack is a cooperative attack which is launched between two malicious nodes. These malicious nodes are distant from each other and each of them sends the received packets to the second peer node through a wormhole tunnel. Then the peer node resends the packets to the original destination. In this way, two malicious nodes seem to be one-hop neighbors and the path which passes through these two nodes looks shorter than the actual path between the source and the destination [4]. Therefore, the mali-

[*] Corresponding author.
Email addresses: `shamaei@ce.sharif.edu` (Sh. Shamaei), `movaghar@sharif.edu` (A. Movaghar).

ISSN: 2008-2045 © 2014 ISC. All rights reserved.

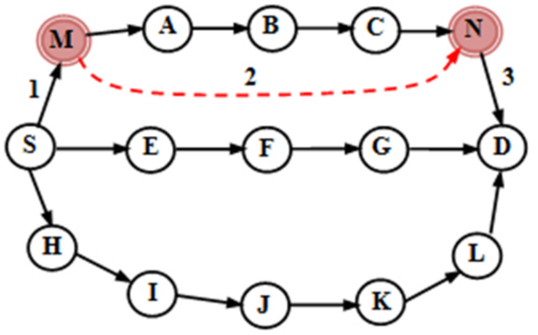

Figure 1. Example of the wormhole attack in MANET.

cious nodes deceive the normal nodes and disturb the routing process [5].

As an example, consider the source node S run a routing protocol like AODV [6], for communicating with the destination node D. If the network is in a normal situation (there is no wormhole attack), the middle path $(S - E - F - G - D)$ is selected in the routing process (Figure 1). Although this path has a length of 4 hops, and it is the shortest path among others, if nodes M and N act as wormhole nodes, a path $(S - M - N - D)$ will be selected in the routing process, which includes the wormhole tunnel. Since the path passing through these two nodes has a length of 6 hops, it appears to be a 3−hop path. Indeed, these two wormhole nodes appear as one-hop neighbors of each other, and they distract the routing process in choosing the shortest path.

According to the tunneling method, a wormhole attack can be divided into two separate types; in-band and out-of-band. In the in-band mode, a wormhole attack establishes a tunnel by packet encapsulation, and in the out-of-band mode, the tunnel is established by creating a direct link between the pair of malicious nodes. Furthermore, this attack can be launched in two separated modes, hidden mode and exposed mode, according to malicious nodes' behavior in the routing process.

In the exposed mode, malicious nodes behave normally and add their ID to the routing packets. In the hidden mode, on the other hand, malicious nodes do not put their ID in the routing packets in order to hide themselves in the routing operation. Hence, they are not enumerated in counting the hops.

As it is mentioned, malicious nodes deceive legitimate nodes by packet tunneling between each other. Although these malicious nodes are distant from each other, legitimate nodes consider them as one-hop neighbors. Therefore, they attract a large percentage of the traffic to the wormhole tunnel by distracting the routing process. Moreover, malicious nodes can launch other attacks such as eavesdropping, replay, black-hole or gray-hole [7], attacks on packets which are passing through the wormhole tunnel [8, 9].

In addition to the aforementioned effects, the wormhole attack can be launched without changing the data packets [10]. Thus, using the cryptography mechanisms is not efficient [11]. According to these reasons, wormhole attack is considered as one of the MANETs security threats whose detection is a serious problem in such networks. Hence, enormous amount of work has been done toward the mitigation of wormhole attack and its countermeasure.

Wormhole attack detection methods can be divided into two categories; securing routing protocols and using security systems or special hardware. In the former, new routing protocols which are secured against wormhole attack are proposed, or the available routing protocols are modified in order to be secured against such an attack [4, 12]. Cryptography mechanisms are often used to secure the routing protocols in these methods. In the latter, security systems are used to detect and prevent wormhole attacks. Furthermore, nodes are equipped with special hardware so that their information can be used during a detection process.

In this paper, a detection scheme is proposed which can detect and prevent wormhole attacks. It works according to two parameters, average hop delay and neighbor's behavior monitoring during data packet forwarding. The proposed scheme is used by all nodes, and it does not need any special hardware or clock synchronization. The proposed scheme detects all types of wormhole attacks such as out-of-band and in-band attacks even in hidden or exposed modes.

Our proposed detection scheme is implemented with NS-2 [13] simulator in a realistic scenario with human mobility. The metrics used to evaluate the performance are false positive rate, false negative rate, energy consumption of a node and attack detection time. According to the simulation results, the proposed detection scheme not only has less false positive rate, false-negative rate and energy consumption, but also it can detect wormhole nodes faster than similar works. Thus, the proposed detection scheme outperforms the similar works in most of these criteria.

The contributions of this paper include:

- The proposed detection scheme, in addition to delay, attends to the monitoring of the neighbor's behavior during data packet forwarding. The reason is that the methods which only attend to delay have high false positive rates, because delay also increase due to network congestion or node movement.
- The proposed detection scheme not only detects

all types of wormhole attacks, but also it can prevent a malicious node from launching a wormhole attack again.
- The proposed detection scheme is independent of the routing protocol which is used on the network.

The rest of this paper is organized as follows: Section 2 provides a brief review on previous works on wormhole attack detection, which is followed by a description of the details of the proposed detection scheme in Section 3. Afterwards, the simulation results are compared with three related works in Section 4. Finally, Section 5 concludes the paper.

2 Related Work

Since this paper focuses on using security systems or special hardware methods, these methods are reviewed in this section.

Packet leash [14] is an approach in which some information is added to a packet header. This information is named leash and has two types; geographical leash and temporal leash. In geographical leash, a sender adds its location and the packet transmission time, in order to restrict the packet transmission distance. In temporal leash, a sender adds the packet transmission time and the expiration time to the packet header in order to restrict packet lifetime. This method requires the time synchronization and a special hardware so to find the geographical location.

DelPHI [15] is an approach which can detect wormhole attack according to delay of various paths. In this method, every available disjoint route between a sender and a receiver is found. Then the average delay per hop of each path is calculated based on their end-to-end delay and hop-count. With this regard, a path is considered as a wormhole infected if its average delay per hop is more than the other. Delphi can detect both hidden and exposed modes of wormhole attack; however, it cannot pinpoint the location of the wormhole nodes. Moreover, it does not work well when all the paths include wormhole tunnel.

NTTM [16] is an approach which can detect wormhole attack based on the calculating the Round Trip Time (RTT) between each node of a route. In this approach each node of a route computes RTT between itself and the destination of the route. Then a source node calculates the RTT between itself and each node of a route according to these RTTs. If the RTT between a pair of nodes is more than a threshold value, it is assumed that there is wormhole attack between these nodes. NTTM has high false positive rate when a link of a route is congested. This is because the end to end delay of the route is increased in congestion.

In [17], a mechanism is proposed which detects wormhole attacks by comparing two types of hop count. One is the advertised hop count, which is extracted from the RREP packet header and the other is the minimum hop count, which is estimated according to the end-to-end delay and the transmission range of each node. A path is considered as wormhole infected only if its hop count is smaller than the estimated hop count. This method has a high false positive rate when the network is congested. This is because the end to end delay of the path is increased in such a situation and the minimum hop count is not estimated accurately.

WAP [18] is an approach which can detect hidden and exposed modes of wormhole attack according to neighbor nodes monitoring. For detecting the hidden mode, each node is made to monitor the behavior of its neighbor nodes when it broadcasts the RREQ packet. A path is considered as wormhole infected, if a node overhears the rebroadcasted RREQ after a specific time (WPT). In case of exposed mode, the source node starts the timer after broadcasting the RREQ packet and waits to receive RREP. This node calculates the average time taken by a packet to traverse one hop. If this average time is greater than WPT, the source node will infer that the route is affected by wormhole attack. In this method overhearing in the routing process causes energy waste, because the routing process is performed repeatedly due to the dynamic topology of the network.

In [19], a method is proposed which attends to the neighbors' behavior in the routing process. In this method, each node keeps some information about all its neighbors from which it listens to RREQ rebroadcast. When a node receives an RREP from another node, it checks whether the node ID is saved or not. If a node ID is not saved, the node will be considered as a suspicious node, and it will be added to the blacklist and future communications through that node will be blocked. This method can detect only out-of-band wormhole, because in this mode, a wormhole node unicasts RREQ to its peer using an out-of-band tunnel. Hence, all its neighbors cannot listen to RREQ retransmission.

In [20], an approach is proposed which detects and prevents wormhole attacks by deploying Intrusion Detection System (IDS) in a number of nodes. The proposed IDS nodes monitor the routing behavior of their neighbor nodes in the routing process and estimate the suspicious value for a node according to abnormal transmissions of RREQ and RREP messages. When the suspicious value of a node exceeds a predefined threshold, the IDS node broadcasts a message through the MANET to isolate the malicious node. In this method, all IDS nodes must sniff all routing messages, so the energy consumption of these nodes is regarded as a challenge.

In [21], an approach is proposed which detects and prevents wormhole attacks by using the digital signature. In this method, only each legitimate node shares a digital signature and knows the signature of all nodes in the network. Each node adds its signature to a packet header before it broadcasts the RREQ message. When a node receives an RREQ message, it verifies this signature with the one stored in its database. A node is considered as a malicious node, if there is no match between the two. In this method, it is assumed the key generation, distribution, and management are done securely.

In [22], a technique is proposed which is based on clustering and digital signature for prevention against wormhole attack. In this method, the network is divided into small clusters. Each cluster has a cluster head (CH) that has the public and private key. Each node sends the RREQ message to its cluster's CH. The CH adds its signature to the received packet header and sends it to the neighbor cluster in order for it to be received by the destination cluster. Each CH checks the validation of the received packet signature. If the signature is valid, the CH will add its signature and this process is repeated as long as the packet is received by the destination node. Wormhole attack is prevented by using this method, because the formation of a wormhole between two CH nodes is assumed impossible. In this method, like the digital-signature-based methods, it is assumed the key management is done securely.

3 The Proposed Detection Scheme

In this paper, each node uses the detection scheme which, in addition to delay, attends to neighbor's behavior during data packet forwarding. In this scheme wormhole attacks can be detected and prevented by executing a two-phase algorithm. These two phases are described in details as follows.

3.1 Phase *I*

Phase I is performed by the source node before data packet forwarding. The purpose of this phase is to calculate the average delay per hop of the selected path in the routing process. Accordingly, the source node calculates the round trip time (RTT) of a path between itself and the destination node. For example, if AODV is selected as the routing protocol, the time period from the sending of the RREQ message to the receiving of the RREP message is considered as RTT by the source node. Then, the source node calculates the average delay per hop (DPH) according to (1).

$$DPH = \frac{RTT}{hop\ count} \tag{1}$$

After this calculation, DPH is compared with a predefined threshold in order to decide whether is there any wormhole attack or not. If DPH is greater than the predefined threshold, the existence of wormhole can be suspected. Hence, the second phase will be performed to confirm the existence of wormhole attack.

This predefined threshold is the maximum time required for a one-hop packet transmission, and its value is determined according to network and nodes conditions.

3.2 Phase *II*

The purpose of this phase is to confirm the existence of wormhole attack on a suspicious path and identify the malicious node. Unlike phase I, in this phase, all nodes on the suspected path engage in the detection process.

The source node starts phase II by sending the promiscuous mode activation packet on the suspected path. This packet is sent for preparing the intermediate node to detect the malicious node and each node is prepared to monitor its neighbor's behavior by receiving one packet.

Next, the source node sends data packets on the suspected path and waits for a specific time to deliver a packet which includes the wormhole node ID. If this time is expired, the source node will assume that the suspected path is safe and it will ask all nodes of the path to disable the promiscuous mode.

During data packet forwarding, each node of the suspected path buffers the IP header of the received data packet. This node enables its promiscuous mode for a limited time, and it monitors neighbor's behavior after data packet forwarding. A node is considered as a wormhole node if the retransmitted packet header does not match the buffered header in specific time duration.

The specific time for the neighbor behavior monitoring is an important parameter. If its value is considered to be small, the false positive rate will increase. On the other hand, if its value is considered to be large, energy consumption and detection time will increase. Accordingly, this time duration must be determined according to network conditions. On the other hand, this duration at least is equal to a round trip time for one hop transmission. Thus, in the present work, its value is considered equal to average delay per hop (DPH), which is calculated in phase I.

When a node finds a wormhole node, it stops forwarding data to this node and it sends a blocking message to the source node in order to isolate the malicious node. When a source node ensures the authenticity of the received blocking message, it stops data flow on this path. Then it broadcasts the blocking message to all nodes in order to cooperatively isolate the malicious node. These nodes will add the malicious node ID to the blacklist after receiving the blocking message. Furthermore, they will remove the malicious node ID from their routing table and then will reject all packets forwarded by the nodes on the blacklist. Therefore, the selection of a path which includes a wormhole tunnel established by the above-mentioned malicious node will be impossible in the routing process. In this detection scheme, an authentication mechanism is required in order to confirm the authenticity of a blocking message and prevent node impersonation.

In this phase, the source node waiting time is assumed twice as a round trip time (RTT) which was calculated in phase I. The reason is that, the round trip time of a packet transmission from a source to a node in a path, is at most equal to RTT. As mentioned before, neighbor monitoring time is equal to DPH. Therefore, if a wormhole tunnel exists in a path, source node can receive detection packet after $RTT + \frac{RTT}{hop\ count}$. On the other hand, when a wormhole tunnel exists in a path, the path length (hop count) is shorter than the actual path. Hence, we assume that the source node waiting time is twice as a RTT.

4 Experimental Results

This section we will first show the experimental results of the performance of the proposed detection scheme, and then compare our proposed scheme with other related works.

4.1 Performance of the Proposed Detection Scheme

This study uses NS-2 to evaluate the performance of the proposed detection scheme. All simulation scenarios include fifty normal mobile nodes, which are randomly distributed over an area of $700m * 700m$ and the transmission range of each one is $100m$. The mobility model of each node follows the levy-walk mobility model [23] in which maximum speed is 30 m/s. Other simulation parameters are shown in the Table 1.

In all of the examined attack scenarios, two wormhole nodes are considered. These nodes have characteristics like other normal nodes and they only establish a wormhole tunnel between themselves in the out-of-band or in-band mode. The two wormhole nodes forward received data packets to its destination through wormhole tunnel in all the scenarios.

Table 1. Simulation parameters

Traffic type	$CBR(UDP)$
Traffic rate	0.1 MB/s
Packet size	1000 $bytes$
Routing protocol	$AODV$
MAC	802.11
Simulation time	$100s$

Figure 2 shows the Packet Delivery Ratio (PDR) versus the traffic load for the AODV protocol and the proposed detection scheme. PDR is defined as the ratio of the data packets received by the destination node to those generated by the source node. In these scenarios two wormhole nodes drop received data packets with a probability of 50%.

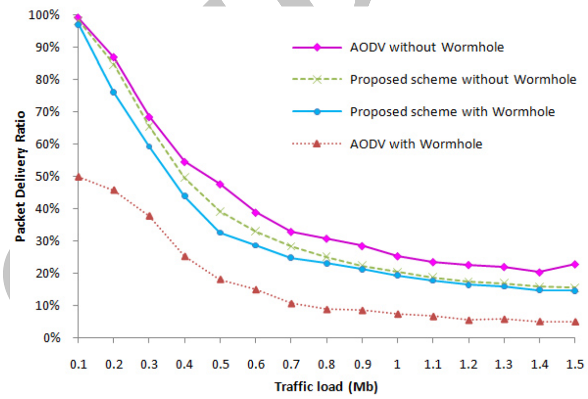

Figure 2. Packet delivery ratio vs. traffic load.

As shown in Figure 2, when there is no wormhole attack on the network, the proposed detection scheme does not reduce the network throughput. The performance of the proposed scheme and AODV is almost the same when traffic loads are low. When traffic load is increased, the PDR of the proposed scheme becomes less than AODV. The reason is that the false positive rate is increased at high traffic loads and accordingly, data flow is stopped by malicious node identifier.

When there is a wormhole attack on the network, performance of the proposed scheme is more than when AODV protocol is used. The reason is that the proposed scheme can block the wormhole node and select another path for data packet forwarding to the destination node. Therefore, the PDR of the proposed scheme is nearly the same as that of a situation without a wormhole attack.

4.2 Comparison between the Proposed Scheme and Related Work

As mentioned in Section 3, the proposed detection scheme detects wormhole attack according to delay and neighbor's behavior. Hence, the proposed scheme is compared to the method presented in [17], which attends to delay. The mentioned method is referred as the detection scheme 3 in this section. Furthermore, the proposed scheme is compared to the methods presented in [18, 19] which attend to neighbors' behavior. These methods are referred as the detection scheme 1 and 2, respectively. False positive rate, false negative rate, energy consumption and detection time of malicious node are the performance metrics, which are used for these comparisons.

4.2.1 False Positive Rate

False positive rate is the percentage of regular links which are falsely detected as wormhole links. Figure 3 compares the false positive rate changes by increasing traffic load of the proposed scheme with the mentioned methods. The purpose of this comparison is to attend to the false positive changes in congestion situation.

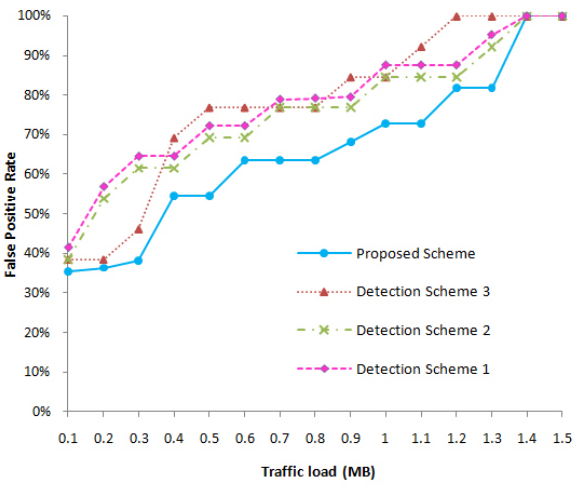

Figure 3. False positive rate vs. traffic load.

As shown in Figure 3, the false positive rate is increased by traffic load increments. The reason is that high traffic load increases packet loss and end to end delay. Hence, delay-based methods and neighbors'-behavior-based methods have high false positive rates in congestion situation.

The proposed detection scheme has a lower false positive rate in comparison to the detection scheme 3 [17], because in addition to delay, it attends to neighbor's behavior. Hence, if a path is considered suspicious due to delay increase, neighbor behavior monitoring will be executed in order to detect the malicious node in phase II. However, in detection scheme 3 [17], if delay of a path increases, it will be considered as a wormhole path.

Moreover, the false positive rate of the proposed scheme is less than those of the detection scheme 1 [18] and the detection scheme 2 [19]. The reason is that these methods monitor neighbors' behavior in all routing processes. Hence, a node is considered malicious whenever a routing packet is dropped because of high traffic load, whereas the proposed scheme will not execute the detection process unless a path is selected in the routing process.

4.2.2 False Negative Rate

In this section false negative rate is studied in order to illustrate the detection capability of the proposed scheme in the in-band and out-of-band mode of wormhole attack. False negative rate is the percentage of infected links which are falsely detected as safe links.

False negative rate of the proposed scheme is zero for various tunnel lengths in the in-band wormhole attack when the first-phase threshold is $4ms$. The reason is that a wormhole node encapsulates the received packets and forwards them to its peer through the intermediate nodes. In this way, the path which passes through two malicious nodes seems to be shorter than the actual path, so the delay per hop of this path will be more than threshold of phase I. On the other hand, a neighbor node does not overhear its packet retransmission because of packet encapsulation. However, false negative rate of detection scheme 3 [17] is nonzero when the wormhole tunnel length is less than four hops. Since the tunnel length is short, there is no more difference between the length of the actual path and the advertised path. Hence, the probability of the advertised hop count being more than the estimated hop count is increased and false negative is increased as well. Furthermore, false negative rate of detection scheme 1 [18] is zero in the in-band wormhole attack, because this method definitely detects abnormal behavior of nodes when a node monitors its neighbors' behavior.

Figure 4 shows the false negative rate in the out-of-band wormhole attack.

In out-of-band wormhole, the false negative rate of the proposed detection scheme is increased when the malicious nodes use a high speed link which has a link delay lower than the first-phase threshold ($4ms$). Because the average delay per hop is less than $4ms$ in this situation, and the infected path is considered as a safe path in the first phase. Whereas, false negative rate of the detection scheme 3 [17] is increased when a high speed link which has a link delay lower than $8ms$ is used by the malicious nodes, because the delay of a wormhole tunnel does not increase end to end delay in this situation. Therefore, the estimated hop count will be equal or less than the advertised hop count and the wormhole attack will not be detected. Furthermore, in the detection scheme 1 [18] and 2

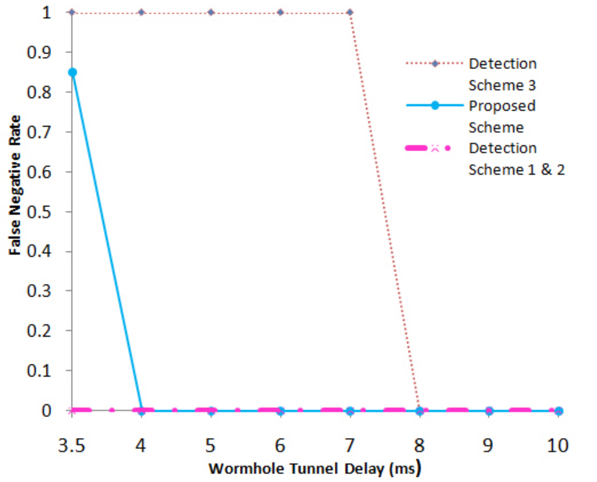

Figure 4. False negative rate vs. out-of-band wormhole tunnel delay.

[19] false negative rate is zero because these methods monitor the behavior of nodes and detect the malicious nodes.

4.2.3 Energy Consumption

As mentioned in Section 3, each node of a suspicious path is set in promiscuous mode to monitor its neighbor's behavior. Since the promiscuous mode consumes a lot of energy, energy consumption of the nodes in the proposed detection scheme is compared to the mentioned methods in this section. In this comparison, the initial energy of each node is considered the same, and equal to 1000 Joule. Figure 5 compares energy consumption of the proposed scheme with the methods presented in [17–19] for the source node. According to these results, energy consumption in the detection scheme 1 and 2 [18, 19] is more than that of other methods. In these methods, all nodes are in promiscuous mode in the routing process. On the other hand, the dynamic topology of MANETs causes the routing process to be done repeatedly. Therefore, nodes will be in promiscuous mode for more time durations, and more energy will be consumed.

Energy consumption of the proposed detection scheme is more than that of the detection scheme 3 [17], since in the proposed scheme, all nodes of a suspicious path must enable their promiscuous mode for specific time duration and monitor their neighbor's behavior.

4.2.4 Detection Time

In this section, the detection time of the proposed detection scheme attack is compared with detection scheme 3 [17]. The reason is that, this scheme detects the wormhole attack after the routing process, as is true in the proposed scheme, while the two other schemes,[18, 19], detect this attack in the routing process. Detection time is considered as the detection time of a wormhole node in this comparison.

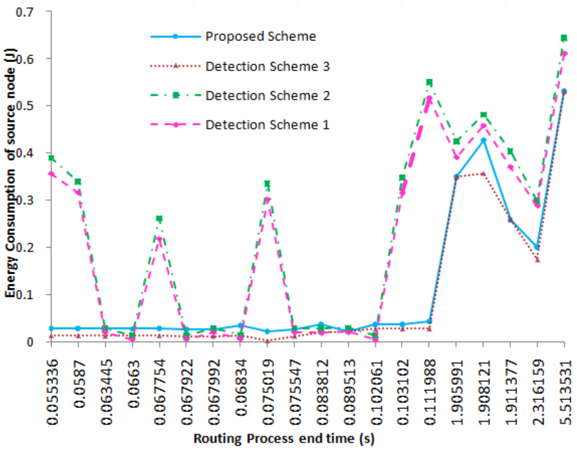

Figure 5. Energy consumption of the source node.

As shown in Figure 6, the proposed scheme detects wormhole node faster than the detection scheme 3 [17]. The reason is that the source node in the detection scheme 3 sends the trace packet on the suspected path, and waits for the reply of each node on the path. The source node calculates the minimum path hop count after receiving a reply of the trace packet from each node. Moreover, the destination node calculates the minimum hop count for each node on the path like the source node to prevent the wormhole nodes from collaborating to deceive the source node. While in the proposed scheme, each node monitors neighbor's behavior as long as the average delay per hop, which is calculated in phase I, and when it finds a malicious node, it immediately informs the source node of this node ID. Accordingly, the detection scheme 3 [17] requires more time to detect the wormhole node in comparison to the proposed scheme.

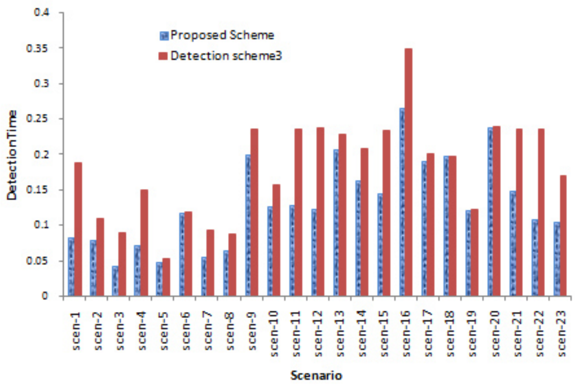

Figure 6. Attack detection time.

5 Conclusion and Future Work

MANETs are vulnerable to various attacks due to the characteristics of both the environment and the nodes. The wormhole attack is one of the attacks which is usually launched by two malicious nodes. These nodes are located far from each other and can disrupt the communications across the network by packet tunneling between themselves. Hence, the detection of wormhole in MANETs is considered as a challenging task.

This paper proposed a detection scheme to detect and prevent wormhole attacks in MANETs. The proposed scheme is based on a two-phase algorithm, which attends to average delay per hop and neighbor's behavior monitoring. According to the simulation results, the proposed scheme is quite well in detecting all types of wormhole attacks without requiring any hardware and clock synchronization and can be integrated into any routing protocol.

In future studies, we plan to improve collaborative communication among malicious node identifier and other nodes in order to improve the performance of the proposed detection scheme. Also, we plan to calculate the computational complexity of the proposed detection scheme.

References

[1] R. Sheikh, M. Singh Chande, and D. Mishra, "Security issues in manet: A review," in *Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On*, pp. 1–4, 2010.

[2] P. Joshi, "Security issues in routing protocols in MANETs at network layer," *Procedia Computer Science*, vol. 3, pp. 954–960, 2011.

[3] S. Banerjee and K. Majumder, "A Comparative Study on Wormhole Attack Prevention Schemes in Mobile Ad-Hoc Network," *In: Thampi, S.M., Zomaya, A.Y., Strufe, T., Alcaraz Calero, J.M., Thomas, T. (eds.) SNDS 2012. CCIS,Recent Trends in Computer Networks and Distributed Systems Security,Springer*, vol. 335, pp. 372–384, 2012.

[4] M.-Y. Su, "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks," *Computers & Security*, vol. 29, pp. 208–224, Mar. 2010.

[5] R. Stoleru, H. Wu, and H. Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks," *Ad Hoc Networks*, vol. 10, pp. 1179–1190, Sept. 2012.

[6] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, pp. 90–100, 1999.

[7] R. Jhaveri, S. Patel, and D. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in *Advanced Computing Communication Technologies (ACCT), 2012 Second International Conference on*, pp. 535–541, 2012.

[8] Supriya and M. Khari, "Mobile Ad Hoc Netwoks Security Attacks and Secured Routing Protocols: A Survey," *Advances in Computer Science and Information Technology. Networks and Communications*, vol. 84, pp. 119–124, 2012.

[9] T. Giannetsos and T. Dimitriou, "LDAC : A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 618–643, 2014.

[10] J. Liu, H. Chen, Z. Zhen, and S. Mingbo, "Intrusion Detection Algorithm for the Wormhole Attack in Ad Hoc Network," in *Proceedings of International Conference on Computer Science and Information Technology*, pp. 147–154, 2014.

[11] J. Zhou, J. Cao, J. Zhang, C. Zhang, and Y. Yu, "Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Testbed," in *26th International Conference on Advanced Information Networking and Applications (AINA) IEEE*, pp. 59–66, 2012.

[12] S. Hazra and S. Setua, "Trusted Routing in AODV Protocol Against Wormhole Attack," *Future Information Technology, Application, and Service. Lecture Notes in Electrical Engineering*, vol. 164, pp. 259–269, 2012.

[13] K. Fall and K. Varadhan, "The ns Manual," *The VINT Project*, 2011.

[14] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, pp. 1976–1986, 2003.

[15] H. S. Chiu and K.-S. Lui, "Delphi: wormhole detection mechanism for ad hoc wireless networks," in *Wireless Pervasive Computing, 2006 1st International Symposium on*, pp. 6–12, 2006.

[16] K. Chanchal and D. Lobiyal, "NTTM : Novel Transmission Time Based Mechanism to Detect Wormhole Attack," *Quality, Reliability, Security and Robustness in Heterogeneous Networks. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 115, pp. 485–495, 2013.

[17] F. Shi, W. Liu, D. Jin, and J. Song, "A countermeasure against wormhole attacks in manets using analytical hierarchy process methodology," *Electronic Commerce Research. Springer US*,

vol. 13, no. 3, pp. 329–345, 2013.

[18] S. Choi, D.-Y. Kim, D. hyeon Lee, and J. il Jung, "Wap: Wormhole attack prevention algorithm in mobile ad hoc networks," in *Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC '08. IEEE International Conference on*, pp. 343–348, 2008.

[19] S. ul Haq and F. B. Hussain, "Out-of-band wormhole attack detection in MANETS," in *the Proceedings of the 9th Australian Information Security Management Conference*, (Perth Western Australia), 2011.

[20] M. Su, "A Study of Deploying Intrusion Detection Systems in Mobile Ad Hoc Networks," *Proceedings of the World Congress on Engineering*, vol. II, pp. 2–6, 2012.

[21] P. Sharma and A. Trivedi, "Prevention of Wormhole Attack in Ad-Hoc Network," *International Journal of Computer Applications Special Issue on Electronics, Information and Communication Engineering - ICEICE*, no. 5, pp. 13–17, 2011.

[22] A. Malhotra, D. Bhardwaj, and A. Garg, "Wormhole attack prevention using clustering and digital signatures in reactive routing," in *Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on*, pp. 122–126, 2012.

[23] S. Rhee, Injong and Shin, Minsu and Hong, Seongik and Lee, Kyunghan and Kim, Seong Joon and Chong, "On the Levy-walk Nature of Human Mobility," *IEEE/ACM Trans. Netw.*, vol. 19, no. 3, pp. 630–643, 2011.

Shiva Shamaei is currently a Ph.D. student in Information Technology Engineering at the Wireless Networking Lab at Sharif University of Technology, Tehran, Iran. She received her B.S. and M.S. degrees in the same field from Isfahan University of Technology, Isfahan, Iran, in 2011 and Sharif University of Technology in 2013, respectively. Her main research interests are mobile ad-hoc networks and their securities.

Ali Movaghar is a Professor in the Department of Computer Engineering at Sharif University of Technology in Tehran, Iran, and has been in the Sharif faculty since 1993. He received his B.S. degree in Electrical Engineering from the University of Tehran in 1977, and M.S. and Ph.D. degrees in Computer, Information, and Control Engineering from the University of Michigan, Ann Arbor, in 1979 and 1985, respectively. He visited the Institut National de Recherche en Informatique et en Automatique in Paris, France and the Department of Electrical Engineering and Computer Science at the University of California, Irvine in 1984 and 2011, respectively, worked at AT&T Information Systems in Naperville, IL in 1985-1986, and taught at the University of Michigan, Ann Arbor in 1987-1989. His research interests include performance/dependability modeling and formal verification of wireless networks and distributed real-time systems. He is a senior member of the IEEE and the ACM.

The ISC Int'l Journal of
Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 198)
http://www.isecure-journal.org

Persian Abstract

یک روش تشخیص دو مرحله‌ای جهت تشخیص حمله‌ی کرم‌چاله در شبکه‌های موردی سیار

شیوا شماعی[۱] و علی موقر[۱]

[۱]دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

حمله‌ی کرم‌چاله از جمله حملاتی است که از مسیریابی توزیع‌شده در شبکه‌های موردی سیار سوءاستفاده می‌کند. در این حمله حداقل دو گره که در فاصله‌ی دوری از یکدیگر قرار دارند با برقراری تونل بین خود، خود را همسایه‌ی یک گامی یکدیگر معرفی می‌کنند. از این رو با فریب سایر گره‌های شبکه منجر به اختلال در فرآیند مسیریابی می‌شوند. به‌علاوه گره‌های بدخواه با ایجاد تونل بین خود بستری برای اجرای سایر حملات فراهم می‌آورند. در این مقاله روش تشخیصی برای این حمله ارائه شده که به دو پارامتر متوسط تأخیر هر گام و رفتار گره‌های همسایه در ارسال بسته‌های داده توجه می‌کند. این روش بدون نیاز به سخت‌افزار اضافی یا همزمان‌سازی گره‌ها قادر به تشخیص تمام حالات حمله از جمله حالات درون شبکه‌ای یا برون شبکه‌ای و حالات مخفی یا آشکار است. همچنین علاوه بر تشخیص حمله، گره‌ی بدخواه را شناسایی می‌کند و از اجرای مجدد حمله توسط آن جلوگیری می‌کند. نتایج شبیه‌سازی نشان دهنده‌ی برتری روش پیشنهادی نسبت به روش‌های مورد مقایسه در این مقاله است.

واژه‌های کلیدی: شبکه‌های موردی سیار، راهکار تشخیص حمله‌ی کرم‌چاله، حمله‌ی کرم‌چاله، تونل کرم‌چاله.