ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

BT-WAP: Wormhole Attack Prevention Model in MANET Based on Hop-Count

Badran Awad[1], Tawfiq Barhoom[2]

Scholar Researcher, Faculty of Information Technology, Islamic University of Gaza, Gaza Strip, Palestine[1]

Associate Professor, Faculty of Information Technology, Islamic University of Gaza, Gaza Strip, Palestine[2]

Abstract*:* MANET has more security issues compared to wired networks. Among all of security threads wormhole attack is considered to be a very serious security thread over MANET. In wormhole attack, two selfish nodes which is geographically very far away to each other, form a tunnel between each other to hide their actual location and try to believe that they are true neighbors and therefore make conversation through the wormhole tunnel. Consequently, the two selfish nodes will completely disrupt the communication channel. In this paper, a new model is developed for detection and prevention of wormholes based hop-count metric which we call it BT-WAP. BT-WAP effectively and efficiently isolates both wormhole node and colluding node. Our model allows the evaluation of node behavior on a pre-packet basis and without the need for more energy consumption or computation-expensive techniques. We show via simulation that BT-WAP successfully avoids misbehaving nodes. It is found that the BT-WAP model achieves an acceptable detection rate about 99.7% and a detection accuracy rate 98.4%. which makes BT-WAP an attractive choice for MANET environments.

Keywords: MANET, wormhole attack, network security, hop-count, range-free, localization.

I. INTRODUCTION

A. MANETs

Mobile Ad hoc networks (MANET) are a new paradigm of wireless communication for mobile hosts (nodes). In an ad hoc network, there is no fixed infrastructure such as mobile switching centers or base stations as shown in Fig. 1. Mobile nodes that are within radio range can communicate between each other, while those that are out of range of wireless link depend on other nodes to relay messages as routers. Node mobility in ad-hoc networks are changing frequently causing changes of the network topology.

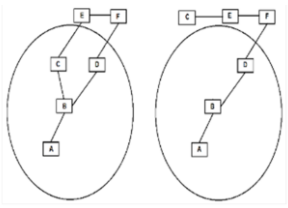

Fig 1: Topology change in ad-hoc

In early days, Ad-Hoc research was mainly focused on military applications, but now MANET's can be used in different applications like conference room, disaster relief, battle field communication and it is also useful, where deployment of infrastructure network is either costly or difficult [1].

MANET is a collection of mobile nodes or devices, such as mobile phones, personal data assistant (PDA), laptops, etc. as shown in Fig. 2, these nodes are connected over a wireless medium [2]. Each node in MANET not only acts as host but also as router that route data from/to other nodes in network.

Use of wireless medium and inherent collaborative nature of the network protocols make such network vulnerable to various forms of attacks. In most wireless networks, an attacker can easily inject bogus packets or impersonating another sender. An attacker can also easily eavesdrop on communication, record packets, and replay the packets that potentially altered [3] [4].

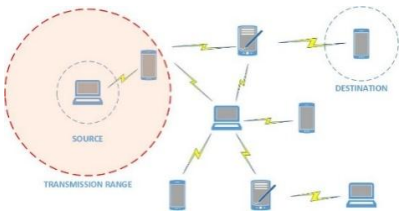

Fig 1: Mobile ad-hoc network

B. MANET'S ROUTING PROTOCOLS

Routing data through a wireless mobile ad hoc network (MANET) is more complex than routing data through a fixed infrastructure based network. The changing topology of MANET requires that the routing protocol be able to manage and adapt the routes in real time. The limited resources of the mobile nodes, both in terms of battery power and network bandwidth, require the routing protocol to be efficient.

MANET routing protocols can be categorized into three types: proactive (table-driven), reactive (demand-driven) and hybrid as in [5] [6].

a. Proactive Routing Protocols

In proactive protocol, every node in a network maintains one or more routing tables that are updated regularly.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Every node sends a broadcast message to the entire network if there is a change in the network topology. But, it incurs additional overhead cost due to maintaining up-to-date information and as a result, throughput of the network may be affected but it provides the actual information to the availability of the network. Destination-Sequence Distance-Vector (DSDV) [7] and Optimized Link State Routing (OLSR) [8] are a proactive protocols.

b. Reactive Routing Protocols

In reactive routing protocol, each node in a network discovers or maintains a route based on-demand. Nodes floods a control message by global broadcast during discovering a route and when route is discovered it is maintained in the temporary cache at a source node unless it is expired or unless link failure happened that requires another route discovery to start over again. Therefore, the main advantage is this protocol needs less routing information but the disadvantages are that it produces huge control packets due to route discovery during topology changes that occurs frequently in MANETs and it incurs higher latency. Currently popular reactive routing protocols are Dynamic Source Routing (DSR) [9] and Ad Hoc On demand Distance Vector (AODV) [2].

c. Hybrid Routing Protocols

Hybrid routing protocols are a mix of table-based and on-demand protocols. These hybrid protocols may be wont to realize a balance between both of the proactive and reactive protocols. Currently, hybrid routing protocols are like, Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR) [10] and Zone Routing Protocol (ZRP) [11].

C. SECURITY ISSUES IN MANET'S

Developing foolproof security protocol for MANETs is tough task [12]. This is mainly because of certain uniqueness of Ad-hoc mobile network, namely, common broadcast radio channel, insecure working environment, lack of central administration and limited availability of resources.

For instance, the early routing protocols, such as AODV and DSR protocols were not designed to provide or guarantee privacy and communication anonymity, rather they were aimed at increasing network performance, efficiency, security, and reliability.

In general, the main security requirements in any system are: confidentiality, integrity, availability. Confidentiality ensures that eavesdroppers will not be able to intercept the information sent through the network which may be achieved by encryption mechanisms. Integrity will insure that packets will not be altered or modified by an adversaries. Finally, Availability implies that the network services must be available to all legitimate users regardless of any malicious events. There are many different aspects to consider in order to classify attacks in MANET's [13]. They can be classified into passive and active attacks depending on how much the attacker is involved. Also, these attacks can be classified depends on the domain of the attack.
They can be classified into internal and external attacks.

D. MANETs ROUTING ATTACKS

A large number of potential attacks exist against MANET routing. These attacks include link spoofing, identity spoofing, man-in-the-middle attack, replay attack, wormhole attack, black-hole attack, routing table overflow attack, Sybil attack, etc. [14]. The purpose of these attacks is to interrupt routing decisions, and to compromise of the communications in order to obtain sensitive information. In fact, MANET's attacks can be divided into two major categories, passive attack and active attack.

Passive attack is eavesdropping of exchanged data done by the attacker without any modification. Therefore, this attack does not disturb the functions of the network. So, this attack violates the confidentiality and analyzes the data that gathered by eavesdropping. In addition, passive attack is harder to detect because it does not affect the network operation. This kind of attacks can be handle by use of an encryption algorithm.

In an **active attack**, the attacker attempts to modify the data that have exchanged in the network. Therefore, this disturbs the operation of network. Active attacks can be divide into two categories as in [15]: In-band and Out-of-band, these attacks shown in the Fig. 3. In-band attacks are most powerful attack because these nodes are actually part of the network, which has all keys and authorization so it is difficult to find it out. Among the many attacks in wireless network attack, a single attacker performs all the attacks mentioned above, but this paper focused on an attack, which is launched by a pair of collaborating attackers: wormhole attack. A wormhole attack is one of the dangerous and specific attacks that the attacker does not require to exploit nodes in the network.

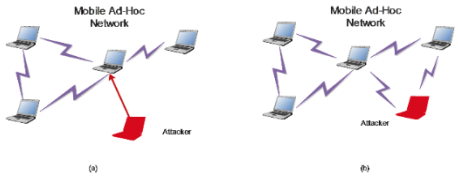

Fig. 2: (a) In-band (b) Out-of-band attacks

E. WORMHOLE ATTACK

Wormhole attack firstly introduced in [16], It's defined as "an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point" as shown in Fig. 4.

The wormhole attack can form a serious threat in wireless networks, especially against many ad-hoc network routing protocols and location-based wireless security systems because it is a passive attack as it does not require the information about the cryptographic infrastructure of the network, hence it puts an attacker in a beneficial or strong position.

a. Wormhole Example

In Fig. 4, an attacker will place two transceivers (nodes) S4 and S8 at two physically different locations in the network as shown.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

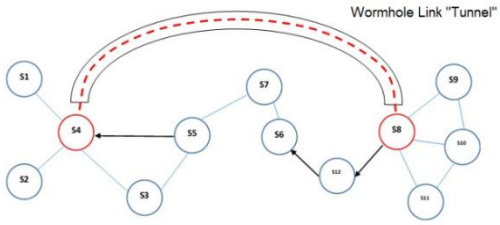

Fig. 3: Wormhole Attack

The nodes S4 and S8 are connected through a wired or long range wireless link called the wormhole link or wormhole tunnel. These nodes capture packets or signals from one location and replay them at the other location. On the other hand, regular nodes controlled by an attacker can be used to tunnel packets from S4 to S8. Legitimate nodes consider the wormhole link as a short path from one side of the network to the other side (e.g., nodes at S4 location in Fig. 4 will assume that nodes at S8 location are one-hop neighbors). Encryption and authentication do not help as the nodes simply relay the encrypted or authenticated packets or signals.

Thus, the wormhole will attract a large amount of traffic between different source and destination nodes in the network. For example, authors in [17] [18] showed that strategic placement of a wormhole, in a network where the nodes are uniformly and independently distributed, on average, can impact about 32% of all communications in that network. The nodes at S4 node location in Fig. 4 and all the surrounding nodes will most likely use the wormhole link to reach the nodes located at S8 node location.

b. Impact of Wormhole Attacks

The wormhole will only peacefully when transport all the traffic from one location in the network to another location that is far away, so it could be useful for the network operation as it will improve the network connectivity. To be known, once the traffic is routed through the wormhole, the adversary will gain full control over the traffic. Then, a malicious actions might done by selectively dropping data packets which will lower the network throughput and later can perform cryptanalysis attacks.

c. Types of Wormhole Attacks

Wormhole attacks were categorized based on the type of links used by S4 and S8 (in-band, or out-of-band) [19] [20]. In-band wormholes usually the adversaries are insider nodes that use the same communication channel used by the other nodes in the network. The nodes will try to increase their transmission range by transmitting at the highest possible power to ensure faster delivery. Furthermore, in out-of-band attacks the adversaries will connect his nodes with long range fast connections and this can be either a long range wireless link that uses a different radio frequency or a fast wired link. Out-of-band wormholes are more advanced and damaging because the longer and faster the wormhole, the more nodes are attracted to send traffic through it and the more damage and disruption it can cause to the network as in [21] [22].

II. RELATED WORK

In literature review, there is many defense mechanisms against the wormhole attack that achieve secure routing protocol. Researchers tried to classify these protocols depending on the technology has been used to secure neighbor discovery and detect wormhole attacks.

A. Time and Location Based Techniques

Hu et al. In [16], suggested a general mechanism of packet leashes – geographic and temporal - to detect wormhole attack introduced. In geographic leashes, node location information is used to bind the distance a packet can traverse. Because wormhole attacks can affect localization, the location information must be obtained via an out-of-band mechanism such as GPS. Further, the "legal" distance a packet can traverse is not always easy to determine. However, in temporal leashes, extremely accurate globally synchronized clocks are used to bind the propagation time of packets that could be hard to obtain particularly in low-cost sensor hardware. But even when available, such timing analysis may not be able to detect cut-through or physical layer wormhole attacks. Therefore, Wormhole attack is detected by detecting the mismatch between the time stamp differences calculated and location difference absorbed.

In [23], an authenticated distance bounding technique called MAD is used. This protocol enables the nodes to determine their mutual distance at the time of encounter. However, they rely on a secure challenge request-response and require accurate time measurements.

In [24], ultrasound technique was used to bind the distance for a secure location verification, which called Echo protocol. Use of ultrasound instead of RF signals as before helps in relaxing the timing requirements, but this technique requires an additional hardware. Therefore, it's impractical and add expense and complexity.

All proposed approaches are discussed above, used special hardware such as GPS [16], directional antennas [25], ultrasound [24], or special RF [23] to detect wormholes. These mechanisms cannot be easily applicable to any ad hoc network and add expense, complexity, and special customization. Thus, it is recommended not to propose mechanisms that rely on additional hardware. Also, some of these mechanisms have their own weakness and usually cannot ensure wormholes detection. Also, the adversary can use adversarial nodes that are equipped with the hardware used by the network nodes. For example, an adversary could also uses ultrasound or any other device, and align it in a way to deceive the detection procedure.

B. Connectivity-Based Techniques

In [26], the authors use only connectivity information to check for forbidden substructures in the connectivity graph. In general, the placement of wormhole affect the connectivity of network by creating long links between two neighbors based on their packet drop pattern and not sets of nodes located potentially far away. As a result, they are able to detect the wormhole attack. However, this method isn't very effective when networks become sparse because not enough connectivity information exists.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

In [27], an effective method called WAP (Wormhole Attack Prevention), which is a graph theoretic framework for modeling wormhole links and deriving the necessary and sufficient conditions for detecting and defending against wormhole attacks was presented. This solution should construct a communication graph that range of the network nodes. Once wormhole node is detected, the source node records them in a wormhole node list. However, the proposed method is based on end-to-end signature authentication of routing packets, consequently, they could cause large overhead and be less accurate compared to those approaches.

In general, the main advantage of the approaches that are based on connectivity of neighbor information is that they do not require any time or location information and do not rely on any additional hardware or location/time information. This mechanisms protecting MANETs from future wormhole attack from the same node. However, this method isn't very effective when network nodes increases because communication overhead.

C. Statistics-Based Techniques

Many disjoint path based techniques have been adopted such as the statistical technique in [18] which is based on multi path routing. This technique uses the relative frequency of each link when discovering routes within the network. The main idea beneath this technique resides in the fact that the relative frequency of a link that is part of a wormhole tunnel is much higher than other normal links. They assume that the wormhole does not exist at the time they gather the statistics. Therefore, this techniques fail in mobility networks like MANET.

DelPHI protocol [28] focuses on the delays due to different routes to a receiver. Therefore, a sender can check whether there are any malicious nodes sitting along its paths to a receiver trying to launch wormhole attacks. The obtained delays and hop count information of some disjoint paths are used to decide whether a certain path among these disjoint paths is under a wormhole attack. However, it cannot pinpoint the location of a wormhole. Moreover, because every node, including wormhole nodes, changes the lengths of the routes, wormhole nodes can change the route length in a certain manner so that they can't be detected.

D. Mix-Mode Approaches

The author [29] has proposed an approach called RTT-TC that is based on topological comparisons (connectivity) and round trip time measurements. They have used the AODV routing protocol. In this tactic, a neighbor list contains two segments: Trusted and Suspected nodes. They used RTT measurements in order to get the suspect list, then use the topological comparison method to find real neighbors from the suspected list. In fact, this approach has a high detection rate and does not need any clock synchronization or special devices but has high message overhead.

The authors in [30] proposed a mechanism called WPAODV, based on location encapsulation, neighbor node and hop count method, to deliver wormhole free path from source to destination by adding further feature in AODV routing protocol which is a threshold calculation that depends on hop-count and neighborhood list. The main advantage of this mechanism that they do not require any time or location information and do not rely on any additional hardware or location/time information. Even so, this mechanisms isn't very effective in sparse networks because the loose of node connectivity.

III. METHODOLOGY AND IMPLEMENTATION

A. Fundamentals

The main concept in detecting presence of wormhole in a network is to find out if node is transmitted out of its transmitting range. This can be found out if the received packet is not one of its neighbors. This mechanism suggests that every node will maintain a neighborhood table.

B. Proposed Model Characteristics

Four main important characteristic of the proposed work:

1. **Localization procedure**: The localization process will maintain every node location for future routing need.
2. **Neighborhood table**: Every node in the network will maintain a neighborhood table which will consists of node ID of the neighbor nodes. As the network we are implementing is a uniform one hence the node will be in set in matrix format hence we can easily get the neighborhood table.
3. **Trust factor**: Each node in neighborhood table given a trust value, it is measures the accuracy and sincerity of the immediate neighboring nodes by monitoring their participation in the packet forwarding mechanism.
4. **Detection and Prevention procedure**: The algorithm detects wormhole node and its colluding node based on intermediate node trust factor value. Then, Wormhole and colluding nodes IDs are now blacklisted.

The picture in Fig. 5 shows how a packet in normal condition transmits from source S to destination D, the packet will not travel out of its transmission range. If a packet from S is received by A or B directly then there is a possibility of presence of wormhole in the network.

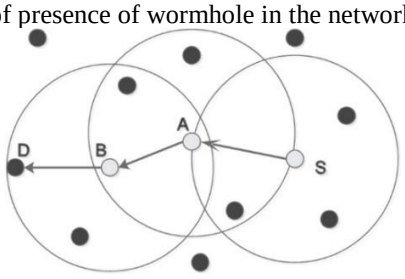

Fig. 4: Normal packet transmission

C. The Proposed Model - General Overview

A general overview of the proposed solution is described in Fig. 6. The proposed solution consists of four steps:

- ***Localization Step***

1. Generate random nodes.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

2. Choose anchor nodes randomly.
3. Localize all nodes using Selective 3-Anchor DV-hop algorithm.
4. Assign a trust value for all of anchors neighbors.

- ***Build Trust Factor Model***

5. Each anchor broadcast "HELLO".
6. Neighbor nodes reply.
7. Each anchor build Neighbor_list (anchor).
8. Compare all anchors' neighbor lists and calculate common nodes.
9. Common nodes assigned TFactor. More common nodes more TFactor.

- ***Route Establishment***

10. Source nodes sends RREQ to all its neighbors.
11. Intermediate nodes forward RREQ until match destination address otherwise repeat until destination not found.
12. Destination node unicast RREP.
13. RREP Contains: hop_count, Neighbor_list(Dest) "Destination's neighbor list"
14. To check wormhole detection go to STEP 17.
15. Rout from source to destination established.
16. Source node stores Neighbor_list(Dest) and hop_count.

- ***Wormhole Detection and Prevention***

17. Check weather Node location within anchor communication Range.
18. If yes, wormhole may exist.
19. Check Neighbour_list(Dest), if node TFactor < threshold.
20. If yes, wormhole exist.
21. Send Announce to all nodes.
22. Any node has wormhole id within Routing_Table, it removes it.
23. Re-initiate route establishment process in STEP 10, to find new route to destination.

IV. RESULTS AND EVALUATION

In this section, an evaluation of the proposed protocol presented. To evaluate proposed model, average hop-count, wormhole detection rate and wormhole detection accuracy rate, an analysis conducted through simulation by presenting proposed model to a non-adversarial models as proposed in most secure routing protocols [31][29][32], and provide a detailed analysis of the obtained simulation results.

A. Simulation Setup

We developed an event driven simulator by using Matlab [33]. The Matlab software used to set up the simulation environment and to visualize the obtained results after computing the actions of all nodes between routing processes.

B. Simulation Parameters

In our simulations, we assumes that physical layer has a fixed communication range pattern,

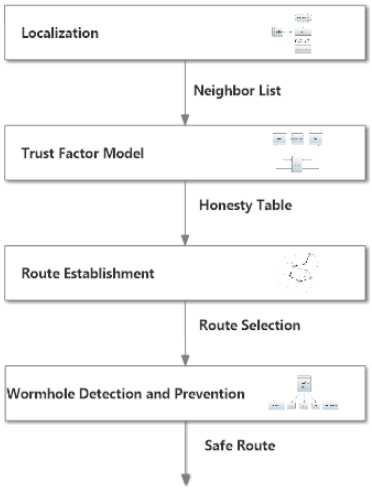

Fig. 5: Proposed model for wormhole detection and prevention

i.e. two nodes can directly communicate with each other successfully only if they are in each other communication range. We randomly deployed 50 nodes within an area of 100 x 100 meters. A fraction of these nodes was randomly selected to wormhole misbehave. The Trust Factor value of each node is initialized to TFactor = 0. Simulations are implemented with 1 source node and 1 destination node. The source node is located at the most left-bottom region of the simulation area, while the destination node is placed at the most right-upper area of simulation environment. This assumption ensures that our results are representative of a long multi-hop path from source to destination; also, it permits potential failures at various distances from the source. Each experiment was repeated for 100 random network topologies. A brief summary of the basic simulation parameters are listed in Table 1 and node random distribution shown in Fig. 7.

Table 1: Simulation parameters

Parameter	Value
Simulation Area	1000 x 1000 (m)
Number of nodes	50
Number of wormhole nodes	1, 2, 4, 8, 16
Communication Range	250 m
Routing Protocol	Modified AODV
Node Speed	10 m/s

C. Performance Evaluation Metrics

The evaluation of the wormhole detection model is measured in accordance to the following three metrics:

- **Average Hop-Count**: Average hop count per route refers to the Total Hop Count of demands over Number of demands as in [34].

$$AverageHopCount = \frac{TotalHopCountOfDemand}{NumberOfDemand} \text{-----(1)}$$

DOI 10.17148/IJARCCE.2015.47134

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

- **Detection rate**: which is the ratio of the number of nodes that are possibly attacked by a wormhole to the number of how many of them are successfully detected as in [31]. Equation 5.2 is used to determine the wormhole detection rate:

$$DetectionRate = \frac{TotalDetectedWormholes}{TotalWormholes} \text{-----(2)}$$

- **Detection Accuracy**: It is the ratio of the number of links declared as attacked by a wormhole to the number of how many of them are actually affected as in [31]. The following formula is used to determine the detection accuracy:

$$DetectionAccuracy = \frac{TotalDetectedWormholes}{TotalActualWormholes} \text{------(3)}$$

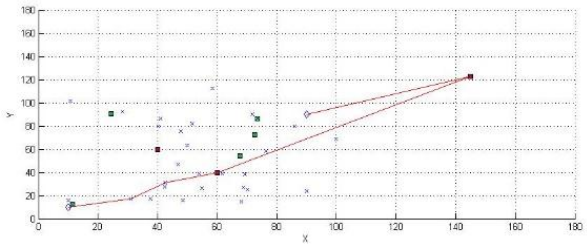

Fig. 6: An environment under Wormhole Attack

D. Experiments Results and Evaluation

In the following graph, Fig. 8, x-axis represents number of nodes and y-axis represents the average Hop-Count. A comparison between number of nodes and the average hop-count obtained for every different scenario presented. We change the number of nodes from 20 to 50. We can find that as the number of wormhole increases, the average hop-count decreases rapidly. Thus, Hop-count metric gives us a good pointer for an existence of wormhole.

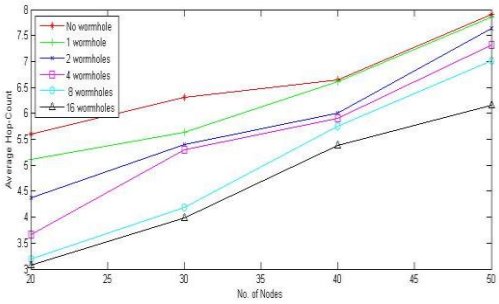

Fig. 7: Relation between number of nodes and number of hop-count

In Fig. 9, the performance of the proposed model is evaluated with Secure-DVHOP routing protocol. The performance of proposed model in this thesis is compared with AODV routing protocol and normal mode without wormhole. No wormhole scenario, in blue line, shows the average route length in normal situation, and it will be used as a reference for the performance of proposed model. With no any detection and prevention to wormhole, the graph shows a decrease in average hop-count. In proposed solution, the graph shows an increase in average hop-count which indicates that now the nodes avoiding malicious path effectively.

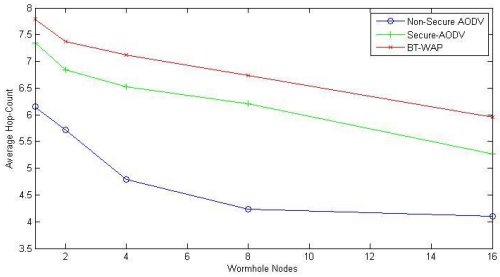

Fig. 8: Number of wormholes vs average hop-count

Fig. 10 shows the wormhole detection rate versus the number of wormholes for AODV routing protocols compared to proposed solution. It can be seen that the wormhole detection rate shows an increasing trend as the number of the wormholes is increased. This is because that with larger wormhole sizes, the probability of the actually attacked neighbors being included in the suspected part of the source's Neighbor-List is almost certain due to the hop-count between them. The detection rate curves are almost bend slightly for larger wormhole sizes because the probability of suspected nodes is much higher than the rate of change in number of one hop neighbors. The proposed model, with blue line, shows better detection rate compared to AODV routing protocol under same network configuration.

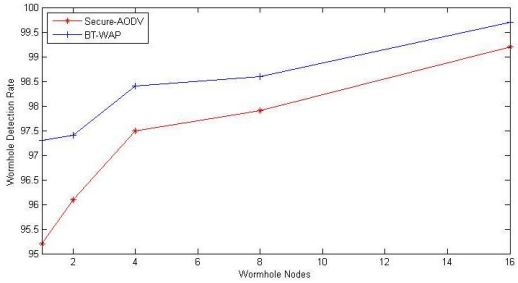

Fig. 9: Number of Wormholes vs Wormhole detection rate

In Fig. 11, a comparison between AODV routing protocol and proposed model presented to show the accuracy of wormhole detection. From the results, it can be seen that our model, with blue line, achieves much higher accuracy of alarms because the number of neighbors that can be selected to form wormhole tunnels by malicious nodes. When the number of wormhole nodes in the network is equal to 1, the number of any node's neighbors is more likely to be small; as the number of wormhole increases, it becomes rarely obvious to find another route similar to that of the detected wormhole tunnel.

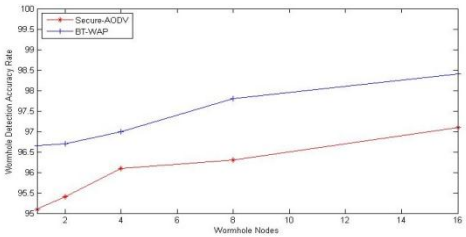

Fig. 10: Number of Wormholes vs Wormhole detection accuracy rate

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

V. CONCLUSION AND FUTURE WORK

Wormhole attacks in MANET significantly degrade network performance and threat to network security. Wormhole attacks are severe attacks that can easily be launched even in networks with confidentiality and authenticity. Malicious nodes usually target the routing control messages related to topology or routing information. In this thesis, we have presented an effective model for detecting and preventing wormhole attacks in DVHOP. To detect wormhole tunnels, we use hop-count metric which inherited from routing protocol. The BT-WAP model is easy to deploy: it does not require any especial hardware, like, time synchronization or GPS; nor does it require any complex computation. The performance of this BT-WAP model shows a high detection rate under various scenarios. BT-WAP model achieves a detection rate about 99.7% versus 99.2% for Secure-AODV model and a detection accuracy rate 98.4% versus 97.1 for Secure-AODV. Our BT-WAP model can be improved by providing custom encryption algorithm that satisfies both integrity and authentication and taking into account the limitations of mobile ad hoc networks as power consumption, computation capability and storage resources.

REFERENCES

[1] Z. J. Haas, "Securing ad hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, 1999.
[2] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," *... WMCSA'99. Second IEEE Work.*, 1999.
[3] J. Kong and X. Hong, "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," *... Int. Symp. Mob. ad hoc Netw. ...*, pp. 291–302, 2003.
[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Mask: Anonymous on-demand routing in mobile ad hoc networks," *Wirel. Commun. ...*, vol. 5, no. 9, pp. 2376–2385, 2006.
[5] K. El Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," *Mob. Comput. IEEE Trans. ...*, pp. 1–14, 2011.
[6] E. Royer and C. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *Pers. Commun. IEEE*, no. April, pp. 46–55, 1999.
[7] G. He, "Destination-sequenced distance vector (DSDV) protocol," *Netw. Lab. Helsinki Univ. ...*, 2002.
[8] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," *IEEE INMIC 2001 IEEE Int. MULTI Top. Conf. 2001, Proc. Technol. 21ST CENTURY*, vol. 1, pp. 62–68, 2001.
[9] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mob. Comput.*, 1996.
[10] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: A core-extraction distributed ad hoc routing algorithm," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 8, pp. 1454–1465, 1999.
[11] N. Beijar, "Zone Routing Protocol (ZRP)," *Networking Laboratory, Helsinki University of Technology, Finland*, pp. 1–12, 2002.
[12] P. Suman and A. Suman, "An Enhanced TCP Corruption Control Mechanism For Wireless Network," *HCTL Open Int. J. Technol. ...*, vol. 1, no. January, pp. 27–40, 2013.
[13] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wirel. Netw. Secur.*, pp. 103–135, 2007.
[14] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," *Commun. Mag. IEEE*, no. October, pp. 70–75, 2002.
[15] R. Siwach and V. Kaul, "A Study of Manet and Wormhole Attack in Mobile Adhoc Network," *... J. Comput. Sci. Mob. Comput. ...*, vol. 2, no. June, pp. 413–420, 2013.
[16] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," *INFOCOM 2003. Twenty- ...*, vol. 00, no. C, 2003.
[17] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols*, 2002, pp. 78–87.
[18] L. Qian and N. Song, "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path," *IEEE Wirel. Commun. Netw. Conf. 2005*, vol. 4, pp. 2106–2111, 2005.
[19] X. Su and R. V. Boppana, "On mitigating in-band wormhole attacks in mobile ad hoc networks," in *IEEE International Conference on Communications*, 2007, pp. 1136–1141.
[20] P. Kruus, D. Sterne, R. Gopaul, M. Heyman, B. Rivera, P. Budulas, B. Luu, T. Johnson, N. Ivanic, and G. Lawler, "In-band wormholes and countermeasures in OLSR networks," in *2006 Securecomm and Workshops*, 2006.
[21] I. Khalil, S. Bagchi, and N. Shroff, "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," *... Networks, 2005. DSN 2005. ...*, pp. 1–10, 2005.
[22] I. Khalil, S. Bagchi, and N. B. Shroff, "MobiWorp: Mitigation of the wormhole attack in mobile multihop wireless networks," *Ad Hoc Networks*, vol. 6, no. 3, pp. 344–362, May 2008.
[23] S. Čapkun, L. Buttyán, and J. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," *... ad hoc Sens. networks*, vol. 67322, no. 5005, 2003.
[24] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," *Proc. 2nd ACM Work. ...*, no. Section 2, 2003.
[25] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," in *Network and Distributed Systems Symposium, NDSS*, 2004, no. February, pp. 1–11.
[26] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," *IEEE INFOCOM 2007 - 26th IEEE Int. Conf. Comput. Commun.*, pp. 107–115, 2007.
[27] S. Choi, D. Kim, D. Lee, and J. Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," *2008 IEEE Int. Conf. Sens. Networks, Ubiquitous, Trust. Comput. (sutc 2008)*, pp. 343–348, Jun. 2008.
[28] H. Chiu and K. Lui, "DelPHI: wormhole detection mechanism for ad hoc wireless networks," *Wirel. Pervasive Comput. 2006 1st ...*, no. 852, 2006.
[29] M. R. Alam and K. S. Chan, "RTT-TC: A topological comparison based method to detect wormhole attacks in MANET," *Int. Conf. Commun. Technol. Proceedings, ICCT*, pp. 991–994, 2010.
[30] R. Shukla, "WPAODV: Wormhole Detection and Prevention Technique," *Int. J. Adv. Netw. Appl.*, 2013.
[31] M. R. Alam and K. Chan, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks," *Inf. Secur.*, no. May, pp. 1–4, 2011.
[32] T. Hayajneh, "PROTOCOLS FOR DETECTION AND REMOVAL OF WORMHOLES FOR SECURE ROUTING AND NEIGHBORHOOD CREATION IN WIRELESS AD HOC NETWORKS by Thaier Saleh Hayajneh BSc EE , Jordan University of Science & Technology , 1997 MS ECE , Jordan University of Science & Technology," 2009.
[33] M. U. Guide, "The mathworks," *Inc., Natick, MA*, vol. 5, p. 333, 1998.
[34] R. Luo, D. Belis, R. M. E. Amiee, and G. A. Manson, "Estimation of average hop count using the grid pattern in multi-hop wireless ad-hoc network," pp. 1–4.

BIOGRAPHIES

Badran Awad, has obtained his B.S. in information and communication technology, from Al-Quds Open University, Gaza in 2010. He is currently pursuing his M.S. in Information Technology from Islamic University-Gaza. His areas of interest include network security, wireless communications and cryptography.

Tawfiq Barhoom, received his PH.D degree from Shanghai Jiao Tong University (SJTU),in 2004.This author is the Dean of Faculty of IT, Islamic University-Gaza, his current interest research include Secure software, Modeling, XMLs security, Web services and its Applications, and Information retrieving.