Detection of Wormhole Attack using Round Trip Time and Node Workload

Bharti Patidar
Computer Science Department
Patel College of Science and Technology, Indore

Reshma Rai Shivhare
Asst. Prof. Computer Science Department
Patel College of Science and Technology, Indore

ABSTRACT
Mobile ad hoc network is one of the most popular research area in wireless network. The properties of node mobility, data relying and administrative control less configuration of network keep attracting researchers. In this network routing is a backbone of control and data transmission methodology, therefore efficient and secure routing techniques is desired. In order to find solution for security and performance in such networks, the proposed study includes the investigation of wormhole attack and their detection techniques. In addition of that, a new technique of wormhole avoidance is proposed which prevent attack deployment and their effect. It also improves the network performance in terms of the packet delivery ratio, throughput and end to end delay in the network.

Keywords
MANET, Wormhole, RTT, Routing Attack, Threshold, Secure Routing.

1. INTRODUCTION
Mobile ad hoc network is a wireless network without any pre-defined infrastructure, in this network the network devices are known as nodes. The connectivity between two network devices is performed using wireless links. These links are fluctuating with the distance between devices. The network devices are able to move independently in the entire network area, thus the network devices are mobile. Due to mobility the network suffers from, performance and security problems.

Wireless mobile ad hoc network simulates some characteristics by which the network is differentiated from the other kind of networks.

1. Each node acts both as a host and as a router.
2. Once a source node and a destination node for a message is out of the radio range, then the network is capable of multi-hop routing.
3. Distributed nature of security, routing and host constitution.
4. The nodes will be a part of or leave the network anytime, making the configuration dynamic in nature..
5. Mobile nodes are characterized by less memories, power and light weight characteristics.
6. The reliability, efficiency, stability and capability of wireless links are typically inferior compared to wired links.
7. Mobile and spontaneous behavior that demands minimum human intervention to configure the network.
8. All nodes have identical options with similar responsibilities and capabilities.
9. High user density and enormous level of user mobility.

2. BACKGROUND
In wormhole attack a malicious device receives packets at one place in the network to another location in the network, where these packets are retransmitted to the network. This channel between two secret agreement attackers is referred to as a wormhole. It could be established through wired links between two secret agreement attackers are using a single long-range wireless connection. In this type of attack the attacker may construct a wormhole for packets not addressed to itself, for the reason that the broadcast property of the radio channel.

For example, in Figure1 X and Y are two malicious devices that wrap data packets and fake the route lengths.

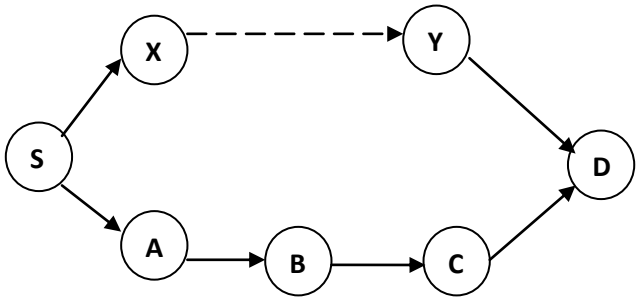

Fig. 1: Wormhole attack

Assume that node S needs to make a route to D and initiate route detection. once X receives a route request from S, X encapsulates the route appeal and tunnels it to Y over an available route, in this situation {X → A → B → C → Y} . Once Y receives the encapsulated route request for D then it will demonstrate that it had only traversed {X → A → B → C → Y}. Neither X nor Y update the packet header. After route detection, the destination finds two totally different routes of unequal length from S: one is about four and another is about three. If Y tunnel the route reply to X, S would incorrectly think about the pathway to D via X is better than the pathway to D via A. Thus, tunneling will stop honest intermediate devices from properly increasing the metric used to calculate path lengths.

While no harm is done if the wormhole is used for efficient routing, it puts the attacker in a strong position as compared to other device in the network, by which an attacker can utilize in a way that could compromise with the security of the network.

The wormhole attack is principally unsecure for various ad hoc network routing techniques by which the device that listen a packet transmission openly from some node, consider themselves to be in the range of (and thus a neighbour of) that node. As an instance, while used against an on-demand routing protocol such as DSR, a strong application of wormhole attack can be raided by tunneling each RREQ packet directly to the target node of the request. When end

node's neighbours find this request packet, they will pursue normal routing protocol processing to rebroadcast that copy of the request and then reject without handling all other received RREQ packets originating from this same route detection. This attack prevents routes other than through the wormhole actually detected, and if the malicious user is near source of the route detection. This attack can prevent routes more than two hops from being discovered. Conceivable manner for the attacker to then abuse the wormhole include discarding rather than forwarding all data packets, thus deploying a permanent DoS attack or selectively discarding or modifying certain data packets. So, if proper mechanisms are not in a job to protect the network from wormhole attacks, most of the active routing protocols for adhoc wireless networks may fail to find valid routes.

In this section recent development in the detection and prevention of wormhole attack models is studied.

Mobile adhoc networks offer a dynamic environment where data exchange and routing between nodes occurs without the assistance of any centralized server or human intervention, providing that nodes work with one another. In such environment, the presence of malevolent nodes could lead to wormhole attacks. In this paper Isaac Woungang et al [1], a secured AODV-based routing theme (TSMI) is planned for mitigating such attacks. Simulation results are provided to demonstrate the effectiveness of their approach, using the packet delivery ratio, the number of broken links detected and number of packets received by destination, as performance indicators.

ZolidahKasiran et al [2] studies the wormhole attack in mobile ad hoc networks and in order to simulate the impact implements a simulation. According to their description the Mobile Ad hoc Networks is a collection of wireless devices that communicate by dispatching packets to one another or on behalf of another device or node, while having not any central network authority or infrastructure controlling data routing. In order to communicate one another, the nodes cooperatively forward data packets to different nodes within the network by using the routing protocol. The simulation result has shown that there is difference performance in throughput when there is an attack.

Delay Tolerant Network is a paradigm developed to cope with intermittent connectivity in wireless networks. Wireless networks are at risk of a range of attacks, including wormhole attack. Thi Ngoc Diep Pham et al [3] propos statistical approach using infrastructure nodes to notice the presence of the wormhole and localize the wormhole endpoints placement. The simulation results demonstrate that their mechanism is simpler than the related method called prohibited topology technique, especially in high-speed network such as vehicular DTNs.

Wormhole switching is a popular switching technique that is additionally vulnerable to deadlocks. Deadlock analysis of routing functions is a manual and complicated task. FreekVerbeek et al [4] propose an algorithm that mechanically proves routing functions deadlock-free or outputs a minimal counter-example explaining the source of the deadlock. Their algorithm is the first to automatically check a necessary and sufficient condition for deadlock-free routing.

The main role of wireless sensor networks is to gather sensor environmental data from monitored area. Because of faults or malicious nodes, sensor data collected or reported might be wrong. Hence it is necessary to detect the presence of wrong sensor readings and deceptive reports. In this paper, Ahmed Louazani et al [5] present a proper model using Time Petri Net to formally evaluate a proposed solution for detecting wormhole attack in CL-MAC, a cross-layer MAC protocol developed at MAC layer for energy efficiency and low latency in WSN. Lunching wormhole attack in CL-MAC will cause the protocol invalid in some situations. Wormhole attack in CL-MAC is discussed, and a formal approach based on Time Petri Net to detect wormhole attack is presented.

3. PROPOSED WORK

In this proposed work the main aim is to find the optimum solution for wormhole detection and prevention additionally, improving the network performance during attack conditions. Thus the following objectives are established.

3.1 Study of Routing based Attack and their Deployment Techniques

In this phase the different kind of routing based attacks and their formation in a wireless network is studied.

3.2 Study of Wormhole Detection and Avoidance Techniques

In this phase the recently developed techniques of wormhole detection and prevention techniques are observed in obtaining secure route between source and destination.

3.3 Implementation of New Improved Secure Route Discovery Technique

In this phase a new routing technique is proposed and implemented using NS2 network simulation environment.

3.4 Performance Analysis and Comparative Study with Existing Technique

After implementation the proposed routing protocol is compared with the previously available secure routing protocol. The comparative study is performed under end to end delay, packet delivery ratio and throughput.

Mobile ad hoc network is a wireless network where the mobility is the key property of the network. Due to mobility the network devices are communicating using multi-hop routing options. In multi-hop routing the network devices relay data to another node and using intermediate nodes the devices transmitting data between source and destination. Thus, during the network path discovery the communication path can adopt new nodes and can leave previous nodes. During this process a malicious node can also join the network and harm the basic functioning of the network. These kinds of attacks are deployed using routing protocols, thus the security for finding a secure path between source and destination is required to develop.

In this domain an essential contribution is provided in [2], the described approach is able to find the malicious attacker efficiently and also can remove the malicious node from network communication. This approach is a kind of watchdog approach for attack detection and prevention. Where for locating the malicious node time based mechanism is discussed. That is the key motivation of the proposed study.

In addition to that there is a number of wormhole detection and prevention techniques are previously developed but most of them are focused on only securing the network from the malicious nodes. Therefore the following issue is considered:

1. The available techniques are issuing additional control messages which can affect the available bandwidth of the network, thus improvement on the available bandwidth is required.
2. The available technique only traces the path for creating decisional threshold, thus a significant amount of delay is produced during secure path discovery, a new kind of method desired which consumes less time for route discovery by which the end to end delay is reduced.

4. METHODOLOGY

In order to find the optimum technique for the wormhole attack detection and prevention a new approach is required to develop for enhancing the network performance and securing the network from attack. A proposal for wireless wormhole detection and routing performance improvement scheme works on the following basic steps:

4.1 Threshold Computation

The threshold values are computed for obtaining a decisional value for finding the secure route between source and destination. Thus a history table is managed, in this history table an ideal network is created and using different sessions the attribute node id, buffer length and propagation delay are observed for creating a threshold value.

4.4.1 Buffer Length

The buffer length of network nodes denotes the computational load on the network node; a less loaded node is efficient for communication in addition of that this node is secure. The threshold value for buffer length is computed as.

$$B_t = \sum_{i=1}^{n} \frac{buffer\ length}{N}$$

4.4.2 Propagation Delay

The during different sessions the transmission delay is computed first as.

$$D_p = \frac{T_d - T_s}{2H}$$

Where Ts is initial time of propagation

Td is time of receiving reply

H number of hop count between sender and receiver

And for computing the threshold the following formula is utilized

$$T_t = \sum_{i=1}^{n} \frac{D_p}{N}$$

Where Dp is delay in propagation

And N is number of nodes

4.2 Secure Route Discovery

The In order to secure a route discovery the two basic constraints are applied to the routing protocol, this results efficient path and secure path between source and destination. That can be taken place in the following manner.

If (node (buffer_length)>Bt&&node (propagation_delay)>Tt)

{

Label node as malicious;

Return;

}

Else if (node (buffer_length) <Bt&&node(propagation_delay))>Tt)

{

Label node as malicious;

Return;

}

Else if

(node (buffer_length)>Bt&&node(propagation_delay))<Tt)

{

Node is legitimate but on high load;

Return;

}

Else if (node (buffer_length)<Bt&&node (propagation_delay))<Tt)

{

Node is legitimate and efficient;

Select node for routing;

}

5. SIMULATION SETUP

This section provides the desired network configuration for simulation of security scheme implementation using AODV routing protocol.

Table 1. Simulation setup

Simulation properties	**Values**
Antenna model	Omni Antenna
Dimension	1000 X 1000
Radio-propagation	Two Ray Ground
Channel Type	Wireless Channel
No of Mobile Nodes	30
Routing protocol	AODV
Time of simulation	30.0 Sec.

6. SIMULATION SCENARIOS

Place In order to simulate the effect of the worm hole attack and the effectiveness of the proposed technique is given using the following simulation scenario:

6.1 Implementation of Traditional AODV Routing

In this experimentation a mobile ad hoc network is prepared and configured using AODV routing protocol. After that a malicious node is deployed on the network and the performance of the routing protocol using the obtained trace file is evaluated.

6.2 Implementation of the Proposed Routing Technique

In this simulation scenario the mobile ad hoc network is configured using the proposed routing protocol. After that a malicious node is deployed over the network and their effect is simulated. Finally the performance of evaluation of the proposed technique is evaluated in terms of throughput, end to end delay and packet delivery ratio.

7. CONCLUSION

Wireless ad hoc networks are keeping attracted researchers for discovering new ways of communication and performance improvement. In this presented work a new secure methodology is developed which secure the network with improving the performance of network. The proposed methodology is works on the basis of decisional threshold which is computed in ideal network conditions. This proposed methodology is optimum for securing the network with performance improvement, in the near future the proposed scheme is implemented using NS2 network simulation environment and their performance is reported. The proposed method is an efficient technique of malicious node prevention in mobile adhoc network.

In near future, it is optimized more for discovering more than one attack in network in addition of that the system is optimized for energy efficiency for a long network life time.

8. REFERENCES

[1] Isaac Woungang, Sanjay Kumar Dhurandher,IssaTraore, Mohammad S. Obaidat, "A Timed and Secured Monitoring Implementation Against Wormhole Attacks in AODV-Based Mobile Ad Hoc Networks", 2013 International Conference on Computer, Information and Telecommunication Systems (CITS).

[2] Zolidah Kasiran and Juliza Mohamad, "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV", ISBN: 978-1-4799-3724-0/14/$31.00 ©2014 IEEE.

[3] Thi Ngoc Diep Pham, Chai Kiat Yeo, "Statistical Wormhole Detection and Localization in Delay Tolerant Networks", the 11th Annual IEEE CCNC - Security, Privacy and Content Protection 978-1-4799-2355-7/14/$31.00 ©2014IEEE.

[4] Freek Verbeek and Julien Schmaltz, "A Decision Procedure for Deadlock-Free Routing in Wormhole Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. 25, NO. 8, AUGUST 2014 1935.

[5] Ahmed Louazani ,Larbi Sekhri,BouabdellahKechar, "A Time Petri Net model for Wormhole Attack Detection in Wireless Sensor Networks",2013 International Conference on Smart Communications in Network Technologies (SaCoNeT).

[6] M. S. Obaidat, I. Woungang, S. Dhurandher, and V. Koo, "Preventing packet dropping and message tampering attacks on aodv-based mobile ad hoc network," in Proc. of the IEEE Intl. Conference on Computer, Information and Telecom. Systems, Amman, Jordan. May 14-16, 2012.

[7] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012.

[8] Saurabh Gupta, Subrat Kar and S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", 2011 International Conference on Innovations in Information Technology.

[9] Vikas Solomon Abel, "Survey of Attacks on Mobile Ad hoc Wireless Networks", (IJCSE) ISSN: 0975-3397 Vol. 3 No. 2 Feb 2011.

[10] Rashid Hafeez Khokhar, MdAsriNgadi, Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", 2008 International Journal of Computer Science and Security, volume (2) issue (3).