International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 6 –OCTOBER 2016 (SPECIAL ISSUE)

An Analysis of Detection and Prevention Methods for Wormhole Attack in MANETs

Pooja A Patil[#1] and Anuradha T[*2]

[#] *PG Student, Dept. of CSE, PDA College of Engg Kalburgi,India*

[*] *Assistant Professor, Dept. of CSE, PDA College of Engg Kalburgi,India*

***Abstract*— Mobile network is a type of adhoc network that can change locations and configuration of nodes in network. Congestion and routing are the common problems faced in mobile network. In mobile network communication is achieved through multi hop hosts with dynamic topology. There are serious security issues in mobile adhoc networks due to its wireless transmissions. The fact that mobile adhoc networks lack fixed infrastructure and use wireless link for communication makes them very susceptible to many malicious attacks. In this paper we discuss the various detecting and preventing techniques for wormhole attacks.**

***Index Terms*— wormhole attack; classification in wormhole attack; routing challenges in wormhole attack.**

I. Introduction

Manet is a infrastructure less, dynamic network, made up of collection of multi hop wireless mobile nodes, that communicate with each other using broadcast mechanism. As Manet is infrastructure less i.e., nodes can be placed anywhere. Due to easy infrastructure setting of Manet, Manets are used in wide verity of application in military, vehicular adhoc networks, civil environment, disaster area, etc.

Each node in Manet work as both router and sensor, in Manet each node has a particular area defined by allocating the range in which the mobile node can send data and receive data. the below figure is representation of mobile adhoc network in which source node connected to destination node through multiple hops and circles represents area of each node.

Current challenges in the MANETS include:

- Quality of service (QOS): Providing a stable QoS for different multimedia services in dynamically changing environment.
- Dynamic Topology: Due to the movement of nodes MANETS are highly dynamic in nature.
- Multicast routing: Designing of multicast routing protocol for a dynamically changing MANET environment.
- Power consumption: Since the nodes in MANET network has Limited battery life and limited processing power so, they have rigorous power requirements.

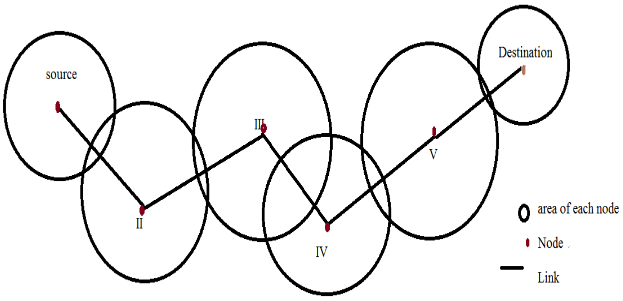


Figure 1.1 mobile Adhoc network

II. Wormhole Attack

Most of routing protocols for adhoc network select cost effective path the nodes participate in routing by forwarding packets to next node till packets reaches to its destination. There are several attacks faced in adhoc networks. Malicious attacks that target dynamic nature of Manet can also be classified by two criteria the mode of attack and attacks on different protocol layers. In passive attack the attackers won’t effect the operation of network. In active attack the attackers effect the operation of network. Wormhole attack is passive attack.

Wormhole attack works by creating a tunnel consists of one or several nodes as relay hops from source to destination, and then broadcast a claim as shortest path in the network to attract the traffic.

The source and destination of tunnel i.e., the two nodes (I and II in figure 2.1)participating in formation of wormhole tunnel are several hops aay from each other , but well connected through a high speed wired or wireless link controlled by attacker.

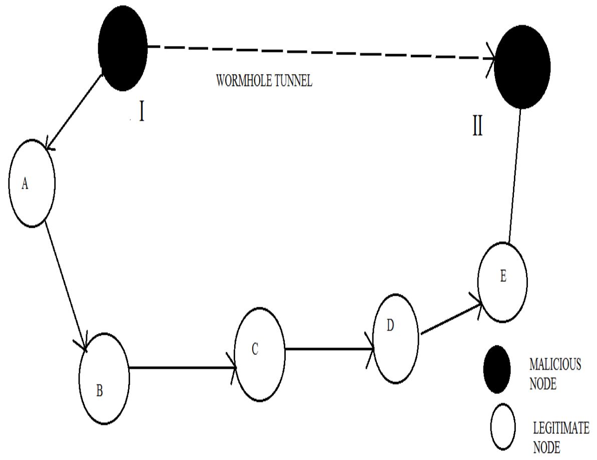


Figure 2.1 wormhole attack

III. TAXONOMY OF WORMHOLE ATTACKS

In literature [1], [2], [3]; wormhole attacks are classified using different criteria. Wormhole attacks can be classified based upon:

A. Its Implementation
B. The medium used
C. The attackers
D. The location of victim nodes.

A. Classification based upon Implementation:

Based upon implementation wormhole attacks can be classified into the following types. This classification relies upon the ways the attack is launched.

A. Using Encapsulation:

In this mode, there are several nodes are involved along the path (nodes along the path may or may not be aware of wormhole) between S and D (as shown in below figure) the packet is encapsulated at S and travels the path in encapsulated form hence avoiding the increase in hop count. The attackers in this scenario are not connected directly to one another but make the other nodes feel that they are directly connected. The packets are transmitted using a virtual tunnel between S and D. Once successfully launched, all paths will contain a link that will comprise of link between S and D.

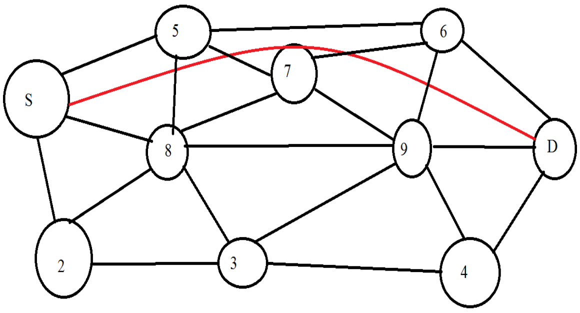


Figure 3.1 In band channel

B. Using Out-of-Band Channel:

The colluder nodes are directly connected through a high bandwidth out of band channel. The channel can be achieved by a wired connection or using a wireless channel which is long range and directional. Due to the requirement of extra hardware it is difficult to launch, but provides an ease because it will not need any encapsulation/decapsulation since the colluders are directly connected.

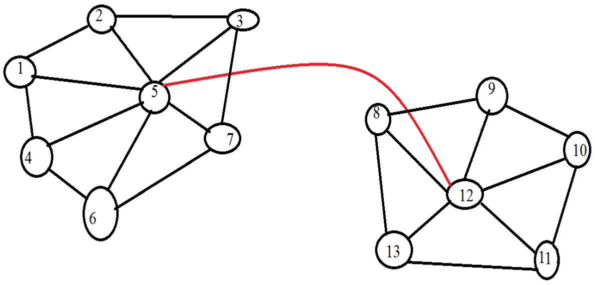


Figure 3.2 out of band channel

1) Using High Power Transmission:

This particular type of wormhole is launched from two colluder nodes that have a high power transmission capability.

2) Via Protocol Deviations:

The attackers in such case create the wormhole by not following the protocol rules, e.g. some of the protocols assume the nodes to wait for some time before retransmitting. But the attackers do not comply with this rule and keeps on broadcasting without back off and thus trying to arrive first at the destination and thereby avoiding any future legitimate requests to reach destination. Even if the future requests reach destination, they will be dropped, since a request passing through the colluder has already been received. Please note that some protocols only anticipate the first request and drops all copies of the same request that arrive in future.

C. Classification based upon Medium Used:

Wormhole attacks can be also classified as In-Band and Out-of-Band wormhole attacks.

1) In-band wormhole:

Attackers are using the same medium for creating link between them e.g. Encapsulation, Packet relay and Protocol deviations.

2) Out-Of-Band Wormhole:

Attackers are not using the same medium as normal network nodes, e.g. Out-Of-Band Channel and High Transmission Mode.

D. Classification based upon Attackers:

1) Self-Sufficient:

Where colluders advertise themselves as normal nodes, all paths passes through them e.g. out-of-band channel or using high power transmission. Our approach focuses on detection of such type of wormhole nodes and attacks.

2) Extended Wormhole:

The colluders are hidden by themselves and extends the attacks beyond themselves to normal nodes e.g. encapsulation or packet relay.

D. Classification based upon location of Victim nodes.

1) Simplex: Victim node lies in range of only one attacker.

2) Duplex: Victim node lies in range of both the attackers.

IV. DETECTION AND PREVENTION TECHNIQUES FOR WORMHOLE ATTACK

Wormhole attack detection is done in two phases [4]. In the preliminary phase of detection, RTT and hop count is used to identify the presence of attack. Once attack is suspected along a route, a Clustering-based approach is done to confirm the presence of attack and localizes the attackers. Clustering-based approach is effective to confirm the presence of wormhole attack with reduced false rate. In the proposed system, wormhole attack detection is done in two phases. In the preliminary phase of detection process, RTT and hop count is used to detect the presence of wormhole attack. Hop count of a route with wormhole link will be very low compared to the actual route to destination. This is because of the presence of high bandwidth optical fibre, which covers a long distance without incrementing the hop count. Since actual distance covered is more, RTT of the route with wormhole attack will be high when compared with a normal route having the same number of hops. In the presence of a wormhole attack, the packets travel more distance along the wormhole link, almost equal to 8 or 9 hops, which will not be added in the hop count of RREP send by the attackers. This distinguishes a normal route from a wormhole link. Once a route is suspected, proposed clustering algorithm is done to confirm the presence of wormhole attack and to localize the attackers. While clustering, every node along the route become the Cluster Head (CH) and groups the nodes into different clusters. After clustering, the source node will confirm the presence of wormhole attack by sending a special control message- Cluster Request (CREQ) to the next node along the route, if that node is a cluster member. Similarly, this CREQ will be forwarded by subsequent nodes along the route until, the next node is no longer cluster member or when destination is reached. At this point, a reply message- Cluster Reply (CREP) having the information about malicious nodes will be send to the source node. The simulation of the proposed clustering algorithm is done using Network Simulator-3 (NS3). Performance analysis of the proposed system is done by comparing the characteristics of normal AODV with the clustering algorithm. The clustering algorithm can effectively eliminate out-of-band wormhole attacks launched by exploiting AODV routing protocol. This clustering-based algorithm can also be extended to detect wormhole attacks in other networks like Wireless Sensor Networks (WSN).

We can also see hop-count analysis and specification based intrusion detection for detecting and preventing wormhole and black hole attacks respectively [5]. Blackhole attack concerns with the network layer of MANET. In black hole attack, an attacker or malicious node aims to consume all the data packets throughout the network. Black hole attack can be of different types depending on aims of the attacker after interception of data exchange between other nodes. Depending on black hole type, after interception of data exchange attacker can either drop all the packets or it can selectively drop packets, or even the malicious node can modify the packets

To evaluate the performance of proposed techniques, simulation of black hole and wormhole attacks along with the simulation of proposed techniques had been done. Simulation of security strategies provides the facility to select a good security solution for routing protocols and gives the knowledge how to use these schemes in hostile and compromised environments. Simulation results show that as the number of nodes increases in the network, the performance of these strategies improves. Nodes mobility affects the performance of routing protocols most.

This techniques show superior performance as PDR and throughput increases however, average end-to-end delay also increases. In the analyzed scenario, it is found that the modified AODV and IDS-AODV has superior performance than AODV. Modified AODV is suitable to detect and prevent wormhole attack. It improves the PDR under attack conditions, with a minimal decrease in throughput and acceptable increase in end-to-end delay. In this simulation study, it has also been investigated that, IDS-AODV is appropriate to detect and prevent black hole attack. It has high PDR and throughput that makes it suitable for networks prone to black hole attack. It provides these advantages with low end-to-end delay.

Routes redundancy and time-based hop calculation for wormhole attacks detection in MANETs [6] are proposed and approach consists of three phase which are routes redundancy, routes aggregation and round-trip-time calculation. It use first phase to create a multipath transmission to ensure that the RREQ is really sent to the destination. Second phase is used to aggregate similar paths including their addresses, so destination and source know every possible valid route that can be used. Last phase is used to calculate the average number of hops according to its round-trip time and investigates the probability of wormhole attackers by comparing number of hops and its average time of every route from the list received by source. All malicious nodes that considered as attackers is isolated and dropped from network. In this scheme does not require additional hardware such as GPS devices and it ensures that request received by destination. Simulation results show this proposed scheme is able to isolate the wormhole attacks and able to hold the increasing of packet dropped compare to AODV approach and time-based calculation.

The method is for combine topological comparison and RTT measurements [7] to detect wormhole attacks. In this section, it presents proposed wormhole detection mechanism. This scheme is based on the following two observations of wormhole attacks:

- Two fake neighbors with a wormhole tunnel in between has longer RTT, compared to the RTT with true neighbors.
- Two true neighbors usually share other true neighbors between them, and two fake neighbors do not share common true neighbors.

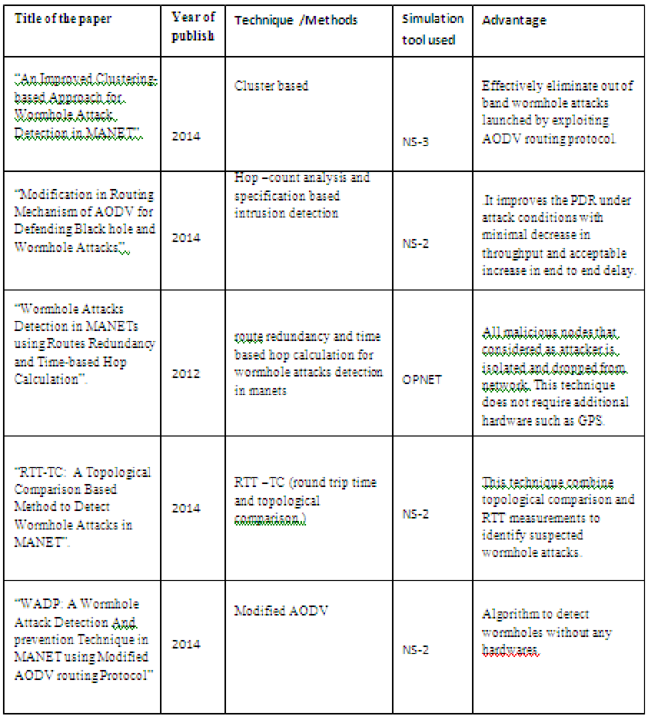
It first relay on RTT measurements to identify suspected wormhole attacks and then use topological comparison to exclude genuine neighbors from the suspected list. Simulation results show that scheme can achieve both high detection rate and accuracy of alarms.

Some modifications have been done in AODV routing protocol [8] to detect and remove wormhole attack in real-world MANET. proposed work, is implemented in modified AODV protocol. Also for removal of false detection we are adding two extra fields in RREP packet that is containing IP of intermediate node and unique number assigned to it. The unique number is a prime number and increments by 19 after every hour. It is assumed that this information is known only to authentic nodes. When a node is unable to specify the right IP and number combination, it is treated as malicious. With implementation of this node authentication test along with WADP in modified AODV, it have a kind of double verification of the presence of wormhole attack. WADP confirms presence of exposed wormhole nodes and node authentication detects it.

V. COMPARISON OF DIFFERENT WORMHOLE DETECTION AND PREVENTION TECNIQUES

This removes false positive problem in WADP also it indicates the exact position of malicious nodes. Node authentication alone can detect exposed wormhole attacks but it can't detect hidden wormhole attacks as when the existence of malicious nodes are unknown then their IP and unique number can't help in detection, therefore , integration of WADP and node authentication in modified AODV protocol removes the short comings of each other. Simulation using ns2 results proves the theory.

.



Title of the paper	Year of publish	Technique /Methods	Simulation tool used	Advantage
"An Improved Clustering-based Approach for Wormhole Attack Detection in MANET".	2014	Cluster based	NS-3	Effectively eliminate out of band wormhole attacks launched by exploiting AODV routing protocol.
"Modification in Routing Mechanism of AODV for Defending Black hole and Wormhole Attacks",.	2014	Hop –count analysis and specification based intrusion detection	NS-2	It improves the PDR under attack conditions with minimal decrease in throughput and acceptable increase in end to end delay.
"Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation".	2012	route redundancy and time based hop calculation for wormhole attacks detection in manets	OPNET	All malicious nodes that considered as attacker is isolated and dropped from network. This technique does not require additional hardware such as GPS.
"RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET".	2014	RTT –TC (round trip time and topological comparison.)	NS-2	This technique combine topological comparison and RTT measurements to identify suspected wormhole attacks.
"WADP: A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol"	2014	Modified AODV	NS-2	Algorithm to detect wormholes without any hardwares.

V. CONCLUSION

Adhoc network is greatly influenced by both active and passive attacks among them adhoc network is highly influenced by wormhole attack. Wormhole attack is one of the most threatening security attacks in mobile ad hoc networks (Manets). Most of the existing solutions for the wormhole attack in MANET suffer implementation difficulty or poor detection performance .In this paper there is a survey on several wormhole detection and prevention techniques .one technique may be different from other. One technique may need special hardware for detecting wormhole attack and other technique may need time synchronization between nodes .The technique to detect the wormhole attack is chosen according to the application where the network is used and based on infrastructure setting of adhoc network

REFERENCES

[1] V. Mahajan , M. Natu and A. Sethi. "Analysis of wormhole intrusion attacks in MANETS". In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

[2] H.S. Chiu and K. Lui . "Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.

[3] R. Maulik , N. Chaki. "A Comprehensive Review on Wormhole Attacks in MANET". In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010.

[4] Anju and sminesh C.N "An Improved Clustering-based Approach for Wormhole Attack Detection in MANET". In 2014 3rd international conference on eco-friendly computing and communication systems.

[5] Kriti patidar and Vandana duby . "RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET". IEEE 2014.

[6] Soo-young shin and Eddy Hartono "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation". IEEE 2012 .

[7] Mohammad Raful Alam and King Sun chan " Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks".In IEEE 2010.

[8] Juhi Biswas , Ajay Gupta and Dayashankar Singh.. dept of CSE, Madan Mohan Maliya University. "WADP: A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol" In IEEE 2014.

[9] Chandandeep kaur and Dr navdeep Kaur "Detection and Prevention Techniques for Wormhole Attacks" In Chandandeep kaur et al, /(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 4926-4929.

[10] [10] E.A.Mary Anita,V.Vasudevan and A.Ashwini, "A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs" IEEE,pp.407-412,2010.

[11] [11] E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj and B.Prabhu, "Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks", IEEE,2011. [

[12] 12] Farid Nait Abdesselam, Brahim Bensaou and Tarik Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", IEEE Communications Magazine , pp.127-133,April 2008.