Detection and Prevention of Wormhole Attack in MANET using New Fresh Algorithm

S.Nivedha, S.SankaraNarayanan

***Abstract*— A Mobile adhoc network (MANET) is a kind of wireless mobile nodes that can communicate with each other through radio waves. It dynamically self-organizes in arbitrary and temporary network topologies. Security is extremely crucial for mobile adhoc networks. Security comes from attacks. If no attacks are there, security is not needed. Among all the potential attacks on mobile adhoc networks, detection of wormhole attack is extremely hard as a result of to launch the attack, One malicious node receives packets from one location, tunnels them to a different malicious node situated in another location of the network and disturb the full routing method. All routes are so directed to the wormhole established by the attackers. The complete routing system in Manet will even be brought down victimization the wormhole attack. We have got surveyed many existing ways to notice wormhole attack in mobile adhoc networks. Our proposed methodology is new fresh wormhole detection and prevention algorithm will effectively notice the worm hole attack in mobile adhoc network. Our goal is to extend the detection quantitative relation compared to existing ways.**

***Index Terms*— Mobile adhoc Network, Wormhole attack, Tunneling, Security, Malicious node, Victimization**

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and hand-held digital devices, It has driven a revolutionary amendment within the computing world. Computing will not just place confidence in the aptitude provided by the non-public computers, and also the conception of present computing emerges and becomes one in every hotspots of analysis within the engineering science society. During this surroundings a route between 2 hosts could contains hops through one or additional nodes within the Manet. A vital downside in an exceedingly mobile adhoc network is finding and maintaining routes since host quality will cause topology changes. Many routing algorithms for MANETs have been projected within the literature and that they take issue within the Manet. New routes are found and existing ones are changed. The mobile adhoc networks are additional vulnerable to suffer from the malicious behaviors than the standard wired networks. Therefore, we would like to pay additional attention to the safety problems within the mobile adhoc networks. The foremost wide thought-about application of a Manet is parcel of land communications. The opposite wide thought-about application for MANETs is interconnection of sensors in associate degree industrial, commercial, or military setting. Another relevant application is that of emergency response. Following are the vulnerabilities of MANET.

(1) Lack of Secure Boundaries
(2) Threats from Compromised nodes Inside the Network
(3) Lack of Centralized Management Facility
(4) Restricted Power Supply
(5) Scalability

There are various attacks in unexpected networks. Attributable to their open nature, mobile adhoc networks area unit liable to many attacks like denial of service, black hole, gray hole, wormhole, Sybil etc. Among all the attacks, detection of wormhole attack is incredibly troublesome because to launch this sort of attack, the offender doesn't want any science break. One malicious node records traffic in one location of the network and tunnels them to a different malicious node that is found far in another location in the network. So whole routing method is disturbed. Detection of such attack is incredibly crucial in mobile adhoc network.

A. Wormhole Attack

The wormhole attack is quite severe, and consists of recording traffic from one region of the network and replaying it in a different region. It is carried out by an intruder. Node *X* is located within transmission range of legitimate nodes *A* and *B*, where *A* and *B* are not themselves within transmission range of each other. Intruder node *X* merely tunnels and control traffic between *A* and *B* (and vice versa), without the modification presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that *X* is virtually invisible.. Node *X* can afterwards drop tunneled packets or break this link at will. Two intruder nodes *X* and *X′*, connected by a wireless or wired private medium, can also collude to create a longer (and more harmful) wormhole. The severity of the wormhole attack comes from the fact that it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are preserved.

Manuscript received June, 2015.
*S.**Nivedha**, Networking Engineering, Kalasalingam University Krishnan kovil, Srivilluputhur, India, Mobile No: 9791819693*
***S.SankaraNarayanan**, Computer Science and Engineering, Kalasalingam University, Krishnan kovil, Srivilluputhur, India, Mobile No: 9976028293*

B. Attacks in Manet

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities

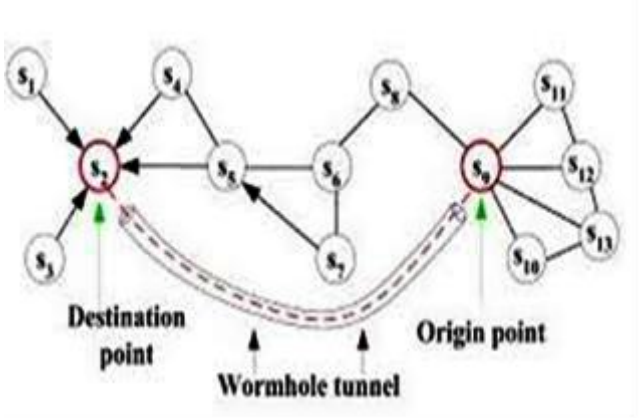


Figure 1: Wormhole Attack

C. Types of Wormhole Attack

By categorizing the attacks into its types makes it easier for its prevention and detection so here wormhole attack has been classified as

a. Open Wormhole attack: In this type of wormhole, the attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbors.

b. **Closed Wormhole Attack:** The attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet.

c. Half open wormhole attack: One side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.

II. PROBLEM STATEMENT

In an ad hoc network, many researchers have worked on detecting wormhole attacks specifically. To defend against them, some efforts are placed on hardware style and signal process techniques. A number of the techniques we have got studied are as follows

A. Packet Leach Approach

The leash is that the information, else into a packet to limit its transmission distance. Within the geographical leashes, the situation information and loosely synchronic clocks along verify the neighbor relation. Each node, before sending a packet, appends its current position and TRM thereto. The receiving node, on receipt of the packet, computes the space to the sender and therefore the time it took the packet to traverse the trail. The receiver will use this distance anytime info to deduce whether or not they received packet more experienced a hollow or not. In temporal leashes, the packet transmission distance is calculated because the product of signal propagation time and therefore the speed of sunshine. In Temporal Leashes, all nodes square measure required to take care of a tightly synchronic clock however don\'t accept GPS information.

B. Time and Trust Based Approach

The technique combines a time-based module with a trust-based module to sight compromised nodes that send false data. These 2 systems run in parallel. Time-based module acts in 3 steps: within the start, neighboring nodes area unit such for every node. In the second step, every node finds the foremost acceptable path to the bottom station. Finally, within the third step, the formula investigates whether or not there's hollow within the network. Malicious nodes on the trail will mislead the time-based module by providing misinformation. To forestall this drawback, trust-based module perpetually observes the primary module and calculates trust values of neighbor nodes. These values area unit accustomed modify the trail next time.

C. Wormhole Attack Prevention Algorithm

All nodes monitor its neighbor's behavior after they send RREQ messages to the destination by employing a special list referred to as Neighbor List. Once a supply node receives some RREP messages, it will discover a route underneath wormhole attack among the routes. Once wormhole node is detected, supply node records them within the hole Node List. Despite the fact that malicious nodes are excluded from routing within the past, the nodes have an opportunity of attack yet again. Therefore, the author stores the information of wormhole nodes at the supply node to participate in routing once more. Moreover, the WAP has the ability of detection each the hidden and exposed attacks while not special hardware

D. Round Trip Time Based Approach

This detection relies on the RTT of the message between nodes. The thought is that the oppose increases the quantity of neighbors of the nodes inside the radius and shortens the trail and longer the RTT worth between successive nodes. Our propose mechanism consists of 3 phases. The primary part is to construct neighbor list for every node and also the second part is to search out the route between sources to destination node. at the moment it finds the hollow link to remove it.

E. Cluster Based Hierarchical Addressing Approach

The receiver will determine whether there is wormhole node is present or not within the routing path and avoid it

throughout the route discovery part. Once receiver receives any packet, it checks the level-1 and level-2 cluster heads ids, and validates the route info hold on within the packet. If the validation is successful then the receiver keeps the packet, otherwise it rejects it. Victimization ranked addressing, the receiver node will verify whether or not the packet has passed from the wormhole tunnel or not.

F. Distributed Algorithm using Graph Information

This Algorithm has delineated the distributed formula for wormhole detection primarily based. The formula relies on unit disk graph assumption, however as mentioned it can even be extended to different cases. in a very unit disk graph, 2 nodes in a very network which square measure distance one apart cannot have over 2 common neighbors that also are distance one except for one another. In different words, 2 freelance (non-neighboring) nodes cannot have over 2 common neighbors that square measure they mutually freelance. However just in case of a hollow attack, nodes within the neighborhood of 1 hollow become neighbors of nodes within the neighborhood of the second hollow and the other way around. Nodes in space A become neighbors of nodes in space B and the other way around.

G. Trust Based Approach

Trust-based theme for distinctive and uninfected nodes that make a hollow within the network. This theme doesn't need any cryptographically means that. During this methodology, trust levels square measure derived in neighboring nodes primarily based upon their sincerity in execution of the routing protocol. This derived trust is then wont to influence the routing decisions. If the trust level is below intensity level then the node is said as compromised node. All the nodes stop communication with this node.

III. Approach

The proposed system considers the problem of preventing the attack for maximum throughput utility in a network with random packet arrivals and time varying channel reliability. The system considers on Hop technique, where each packet requires transmission over a single link.

A. AODV route setup procedure

In AODV, once a node desires to speak with another node and there\'s no valid route in its routing table, it broadcasts a route request packet (RREQ). A node receiving a RREQ for the primary time can setup a reverse route to the supply node in its routing table. If the node is that the destination or encompasses a valid route to the destination, it wills unicast a route reply RREP along the reverse route back to the supply node. Otherwise, it will increase the hop count within the RREQ by one and forward the RREQ to different nodes.

B. New Fresh Algorithm

Step 1:
Whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes. RREQ packet contains destination address and sequence number along with source address. Sequence number provides the freshness of route.

Step 2:
Once an RREQ packet is received by an intermediate node and verifies destination address. If the destination address not matches with the RREQ packet then forwards it to its next hop. This process is repeated until it reaches the final destination.

Step 3:
Route path nodes are saved in routing table.

Step 4:
When source node starts sending packets, it sends to next node and that node sends to next until it reaches destination. The traversed path nodes are checked with the path nodes in routing table.

Step 5:
If the traversed path nodes are not in the routing table, wormhole is detected and it is out band wormhole.

Step 6:
While sending packets to next neighbor node, PDR is calculated for each node. The ratio of sent packets to received packets is calculated for each node.

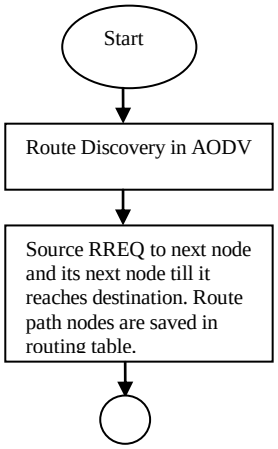
Step 7:
Hello packets are also sending to each node along with packets until it reaches destination. Roundtrip time is calculated for each consecutive node. If the roundtrip time is less than threshold, that link is high speed link and the two nodes are malicious and detected as wormhole. And also if the PDR is less than 1, that node is wormhole node. The wormhole detected is active wormhole as it affects the packets.

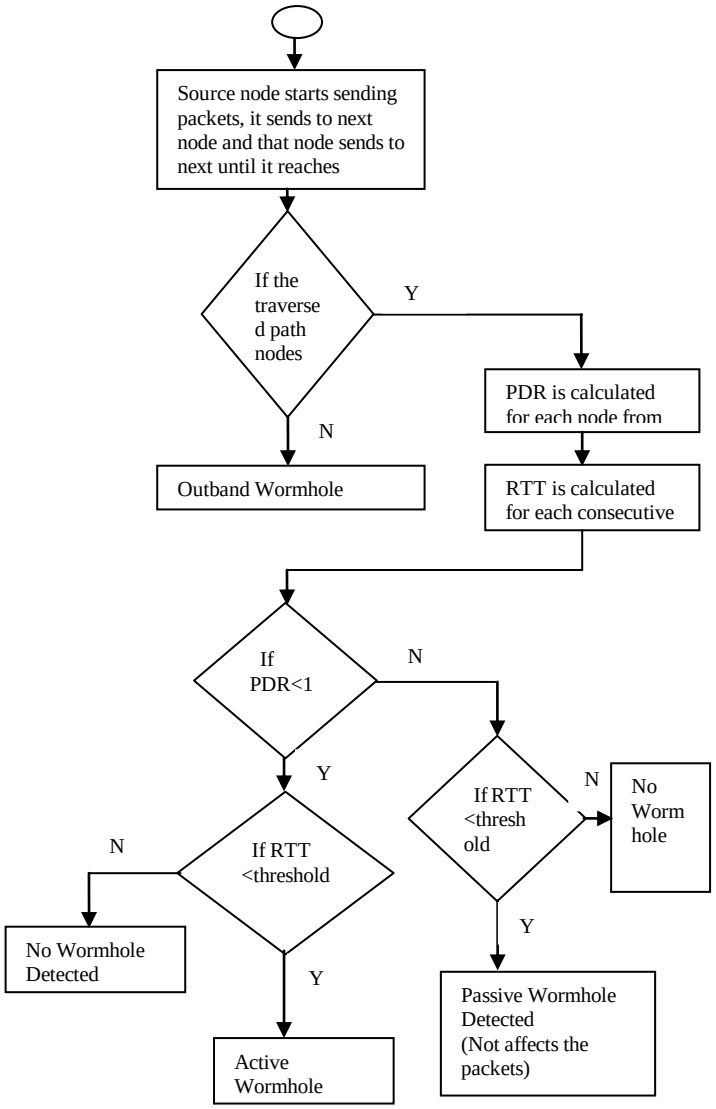
Step 8:
If PDR less than 1 and RTT is not less than threshold means the loss may be due to traffic.

Step 9:
If PDR not less than 1, check for RTT less than threshold or not. If it is less passive wormhole is detected as the packets are not affected. If it is not less than threshold, there is no wormhole.

Step 10:
Wormhole nodes are announced to all other nodes. All nodes remove wormhole node id from its neighbor table and Routing Table. If any forwarding node receives the wormhole announcement node, it will send RERR message to source. It will reinitiate route discovery process, and find the new path to the destination without wormhole node.

C. Flow Chart of New fresh Algorithm





D. Detection of Outband Wormhole Attack

- Whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes.
- If the destination address not matches with the RREQ packet then forwards it to its next hop. This process is repeated until it reaches the final destination.
- When source node starts sending packets, it sends to next node and that node sends to next until it reaches destination. The traversed path nodes are checked with the path nodes in routing table.
- If the traversed path nodes are not in the routing table, wormhole is detected and it is out band wormhole.

E. Detection of Active and Passive Wormhole Attack

- While sending packets to next neighbor node, PDR is calculated for each node. The ratio of sent packets to received packets is calculated for each node.
- Hello packets are also sending to each node along with packets until it reaches destination. Roundtrip time is calculated for each consecutive node.
- If the roundtrip time is less than threshold, that link is high speed link and the two nodes are malicious and detected as wormhole.
- And also if the PDR is less than 1, that node is wormhole node. The wormhole detected is active wormhole as it affects the packets.
- If PDR not less than 1, check for RTT less than threshold or not. If it is less passive wormhole is detected as the packets are not affected. If it is not less than threshold, there is no wormhole.

F. Prevention of Wormhole Attack

- Wormhole nodes are announced to all other nodes. All nodes remove wormhole node id from its neighbor table and Routing Table.
- If any forwarding node receives the wormhole announcement node, it will send RERR message to source.
- It will reinitiate route discovery process, and find the new path to the destination without wormhole node.

IV. Simulation Analysis

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

The simulation study is performed using the NS2 simulator. Performance of New Fresh algorithm is analyzed and graph is depicted in the presence of 50 nodes including malevolent nodes and target. Here we analyzed some performance metrics such as packet delivery ratio, throughput, simulation time, end to end delay and speed. The simulation parameters are shown in the table.

PARAMETER	**VALUE**
Quantity of nodes	50
Area-X	800 m
Area-Y	800 m
Traffic model	CBR
Mobility model	Random way point
Routing protocol	DSR
Packet sending rate	4.0
Packet size (byte)	128
Simulation time	1000 sec
MAC	802.11
No, of malicious nodes	2
Transmission range	40-50 m

Table 1: Experimental setup in NS2

A) Packet Delivery Ratio

Packet delivery ratio is the proportion of the total amount of packets reached the receiver and amount of packet sent by the source.

PDR = Total amount of data packet received (Receiver) /Total amount of packet sent (Source).

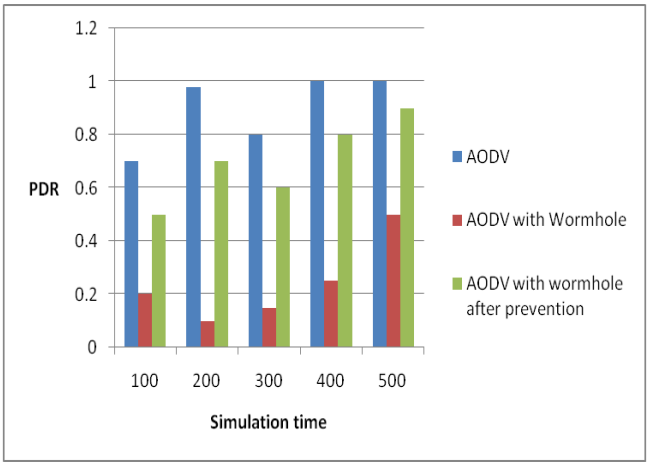


Figure 2: Simulation time (ms) vs. Packet delivery ratio (%)

B) End-to-End Delay

Average End-to-End delay is the average time of the data packet to be successfully transmitted from source to destination. It includes all possible delays such as propagation delay, queuing delays, process delays, etc. A small average End-to-End delay means faster data transmission. Average delay presented by proposed protocol

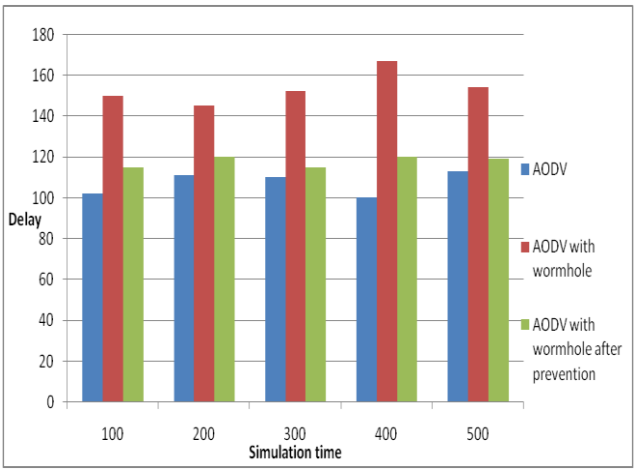


Figure 3: Simulation time vs. Delay (sec)

C) Throughput

Throughput refers to the Ratio of total number of bytes transferred per second.

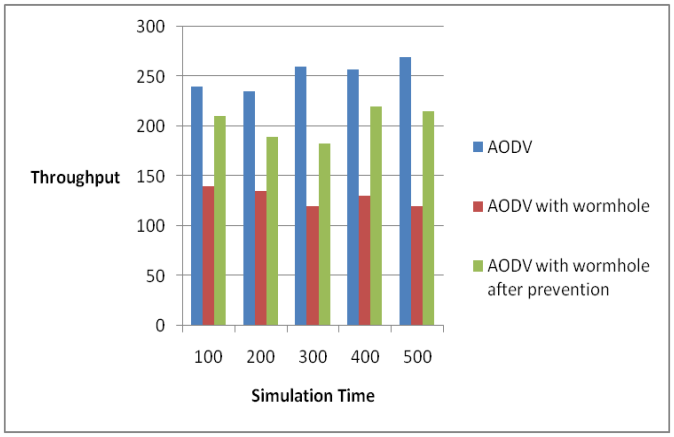


Figure 4: Simulation time vs. Throughput (kB/s)

V. CONCLUSION

In this paper, we focused on detection and removal of wormhole attack during data transmission. The proposed algorithm provides more security to ad hoc networks and also prevent from such kind of attacks. It helps to increases the packet delivery ratio and reduces the control overhead by improving the performance of the routing protocol.

In future, we also plan to improve the table entries at destination node to get the detection of wormhole nodes faster. And also improve the security of wireless ad hoc networks. By deploying such efficient methods to prevent DoS attacks and hybrid attacks with the help of new fresh algorithm.

ACKNOWLEDGMENT

We would like to sincerely thank Assistant Prof. S.SankaraNarayanan for his advice and guidance at the start of this article. His guidance has also been essential during some steps of this article and his quick invaluable insights have always been very helpful. His hard working and passion for research also has set an example that we would like to follow. We really appreciate his interest and enthusiasm during this article. Finally we thank the Editor in chief, the Associate Editor and anonymous Referees for their comments.

REFERENCES

[1] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In IEEE WCNC 2005, Seattle, WA, USA, 2005; pp. 1193–1199.

[2] Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In Dependable Systems and Networks (DSN), pages 612–621, Jun 2005.

[3] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In Proceedings of the Network and Distributed System Security Symposium. 2004.

[4] Subhashis Banerjee1 and Koushik Majumder, "A Novel Custer Based Wormhole Avoidance Algorithm For Mobile Adhoc Networks" David C. Wyld (Eds): ICCSEA, SPPR, CSIA, WimoA – 2013

[5] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks,"(manuscript in Turkish), in 3rd Information Security and Cryptology Conference (ISC ´ 08), pp. 139−4, 2008.

[6] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, Xiangke Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks" IEEE 2009.

[7] Radha Poovendran • Loukas Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks" Springer Science, Wireless Netw (2007).

[8] I.Khalil, S.Bagchi, N.B.Shroff, "A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", In Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN"05).

Author Profile

S.Nivedha is currently a PG scholar in Network Engineering from the Department of Computer Science and Engineering at Kalasalingam University, Krishnan kovil, Srivilluputhur and Tamilnadu. She received his Bachelor Degree in Information Technology from Karunya University, Coimbatore and Tamilnadu. Her Research areas include Networking and Network Security

