Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET

Devendra Singh Kushwaha
M Tech. scholar
Department of CSE
RITS, Bhopal

Ashish Khare
Associate professor
Department of CSE
RITS, Bhopal

J. L .Rana, PhD.
Professor
Department of CSE
RITS, Bhopal

ABSTRACT
Mobile ad hoc networks are comprised of nodes that must cooperate to dynamically establish routes using wireless links. Routes may involve multiple hops with each node acting as a host and router. Since ad hoc networks typically work in an open un-trusted environment with little physical security, they are subject to a number of unique security attacks like wormhole attack. The wormhole attack is considered to be a serious security attack in multi-hop ad hoc networks. In wormhole attack, attacker makes tunnel from one end of the network to the other, nodes stay in different location on two ends of tunnel believe that they are true neighbours and makes conversation through the wormhole link. Unlike many other attacks on ad-hoc routing, a wormhole attack cannot be prevented with cryptographic solutions because intruders neither generate new, nor modify existing, packets, but rather forward existing ones. In this paper a simple technique to effectively detect wormhole attacks without the need for special hardware and/or strict location or synchronization requirements is proposed. The proposed technique makes use of variance in routing information between neighbours to detect wormholes. The base of dissertation is to find alternative path from source to second hop and calculate the number of hops to detect the wormhole.

Keywords: Adhoc network, wormhole, threshold, AODV.

1. INTRODUCTION

Wireless network refers to a network, in which all the devices communicate without the use of wired connection. Wireless networks [1] are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network. Mobile ad hoc network is a part of wireless network [2] which is a self-configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management.

The wormhole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the wormhole attack in MANET a technique has been proposed. In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network [3]. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. In the reactive routing protocols such as AODV, the attackers can tunnel each route request packets to another attacker that is near to destination node [3,4]. When the neighbors of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process.

As mentions in above paragraph wormhole attack have a best impact on the network, it must attract a large amount of network traffic which is done by giving a shortest route to destination in the network. Therefore, the routes going through the wormhole must be shorter than alternate routes through valid network nodes.

Also it is seen that most of the previous approaches for detection of wormhole shows dropped performance and have relative higher complexity [5,6,7,8,9]. As the mobile nodes operate on the limited power of battery therefore it becomes very necessary to develop a technique which can successfully defend against wormhole attacks while maintaining lesser complexity [10,11,12,13]. The objective of this dissertation is to develop a new approach which can successfully defend against wormhole attacks.

2. PROPOSED SOLUTION

The basic idea of the technique is to discover alternative routes to a target node T that is one-hop neighbor’s nodes that do not go through the wormhole. These alternative routes will be extensively dissimilar in length, means the length of the alternative path is greater than the path that have wormhole, and otherwise the wormhole will not attract large amounts of traffic. Consider a communicating source-destination node pair (S, D), with source route PS, D. If node S want to detect the existence of a wormhole, S would find out a new route to T and if the length of the new route differs extensively compared to the length of PS,T (i.e., greater than a threshold), it is concluded that wormhole exists.

Consider a situation in which the source route found by any routing protocol is S->1->2->3->4->5->6->7->8->9->D (as shown in figure 1) which is the legal path.

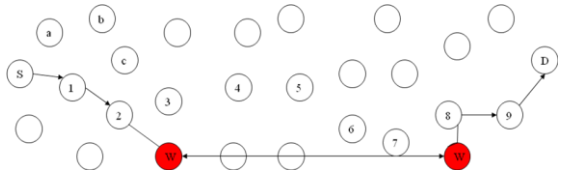

Figure 1Legal source route found by routing protocol

With the introduction of closed wormhole attack in the legal source route, the new malicious route will be S->1->2->8->9->D.

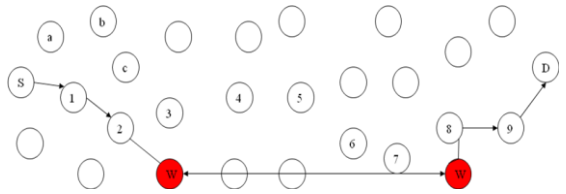

Figure 2 Malicious route containing Wormhole

As the proposed approach for detection of wormhole solely depends on the density of nodes in the network, therefore the value of threshold must be predefined. The threshold value is calculated by checking the average number of hops between the nodes in the network. In the situation defined in figure 2, the value of threshold is calculated as X.

Now in order to detect the wormhole, the proposed approach attempts to find the number of hops on the second shortest route between two alternate nodes starting from the source S. If number of hops in the second shortest path is greater that the predefined threshold, then it is declared that the wormhole is present between the two nodes.

For example the malicious path containing the closed wormhole is S->1->2->8->9->D. Now proposed algorithm will check the number of hops found in the second shortest path between the nodes S and 2. In the situation given in figure 2, second shortest path between S and 2 will S->a->b->c->2. Now the number of hops between S and 2 is found to be 3 which is less than predefined threshold (i.e. X), it is declared that no wormhole is present between the nodes S and 2.

The same algorithm is followed by next two nodes (i.e. 1 and 8). As the number of hops in the second shortest path from node 1 to 8 is greater than the predefined threshold, therefore it the presence of wormhole is declared between the nodes 1 and 8.

Working Framework:

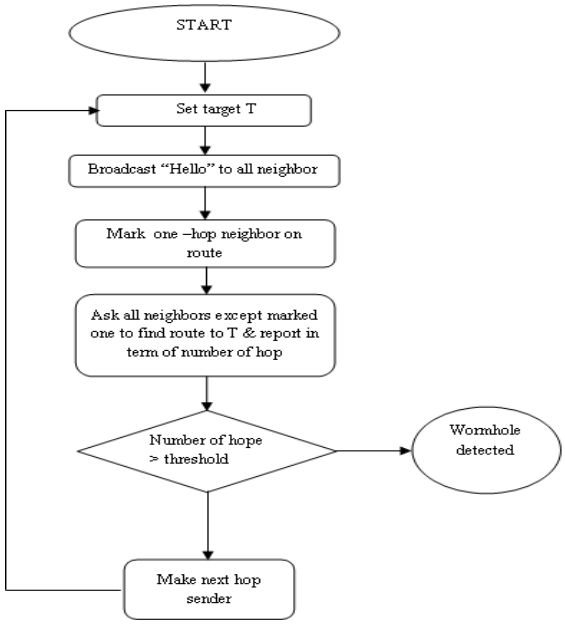

Figure 3 Flowchart of Proposed Algorithm.

3. PROPOSED ALGORITHM FOR THRESHOLD

Threshold is an important part of the proposed technique. In the technique a wormhole tunnel present in the network or not, is decided by the threshold. If the value of alternate path is greater than the threshold, the wormhole is detected. For deciding the threshold considers a network with n number of nodes. In the network, each and every node finds the all alternate route to its neighbor's node. Then find average of greatest of shortest path of minimum number of hop count of each and every alternate path is taken by the routing algorithm. After that our proposed algorithm considers that average number of hop count which is comes from these various alternate paths in the whole network as threshold.

Algorithm: Assumptions

1. Total number of node in desire network is TN.
2. Si represent any node among TN, where i = 1, 2, 3,……., < TN.
3. (RSi)j represent the node that's come in the range of Si.
4. ((RSi)j)k represent the node that's come in the range of (RSi)j and assume as a target node Tjk for Si.
5. PST represent path between S and T.
6. NSi represent the neighbor node of Si.
7. (lNSi,Tjk) represent number of node in the path PNSi,Tjk.

Algorithm (T (N))

For (S_i=1; i<=T; i++)
{
T ($P_{Si/NSi}$) = 0
For (NS_i=1; NS_i<=T (NS_i); NS_{i++})
{
$P_{Si/NSi}$ ←P_{ST}
New (T ($P_{Si/NSi}$)) ←($P_{Si/NSi}$)
If ((T ($P_{Si/NSi}$)) < New (T ($P_{Si/NSi}$)))
(T ($P_{Si/NSi}$)) = New (T ($P_{Si/NSi}$))
}
}
T (N) = ∑T ($P_{Si/NSi}$)

4. Route Discovery Phase

A node broadcasts a RREQ when it determines that it needs a route to a destination and does not have one available (figure 4). This can happen if the destination is previously unknown to the node, or if a previously valid route to the destination expires. To prevent unnecessary broadcasts of RREQs the source node uses an expanding ring search technique as an optimization.

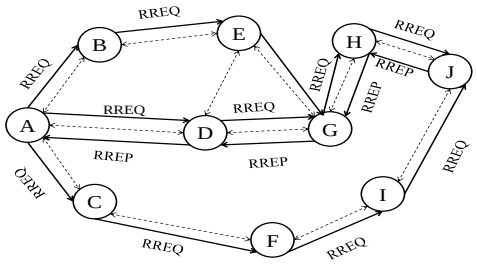

Figure: 4 A possible paths for a route replies if A wishes to find a route to J

5. IMPLEMENTATION OF PROPOSED APPROACH

Wormhole attack implementation:

To implement wormhole attack, the aodv.cc file has been modified. When the simulation starts function named "command" is invoked. All the modification related to the wormhole is done in this function. Functionality to create wormhole nodes by reading the node ID from the file is added in this function. The Tcl script calls this function to create wormhole in the simulation. Tcl also calls the attacking and detecting time, from its related file that is reside in the "command" function.

Detection of wormhole attack:

The algorithm works on the concept of finding the alternate path to the target node. For implementation of this concept, some functions are implemented in aodv.cc file.
First checkpath() function is used to find a true path to the destination, for this function uses two other functions named sendroutemsg() and recvroutemsg().After that a function is needed to set the target node. For this purpose nb_insert() function is created, this function is used to set the value of target node that is a two hop neighbor.

Scenario:

In order to validate the proposed approach a number of simulation experiments have been performed by using network simulator version 2.32. Table 1 show the parameters used in the simulation experiments. The proposed approach is tested with wormhole using a rectangular scenario of 1000 × 1000 m square area; CBR (Constant Bit Rate) traffic is used to generate UDP packets for the simulation. In the simulation, start on 0ms and end on the 100ms. The attack will start on 25ms in the simulation and re-check on 50ms. There are different packets sizes are used in the NS-2, for this simulation 1024KB packet is used. In the simulation the carrier sensing power is defined as 200m.The wormhole is randomly created somewhere between the sender and the receiver with a random length that is uniformly distributed between the nodes. The algorithm is implemented by modifying the original AODV source code in NS-2.

Simulation Area	1000mx1000m
Number of Nodes	Vary from 40 to 100
Communication Traffic	CBR
Simulation Duration	100 Seconds
Packet Rate	1024 kbps
CS Threshold Used In Normal Nodes	200 Meter
RX Threshold Used In Normal Nodes	200 Meter

Table 1 Simulation Parameters

6. SIMULATION AND RESULT ANALYSIS

The performance of the algorithm is studied through a number of simulation tests for network. Different numbers of nodes in each scenario and wormhole tunnels have been generated for the simulation. The simulation results show that the detection technique depends on the network density. Threshold that is considered for wormhole detection also depends on the network density. For the true detection of wormhole, proposed technique compares the hop count with the threshold. So the threshold is an important factor of simulation. If the value of threshold small than the hop count, it will give a higher value of false negative rate (that means it give true alternative route as a false route) and if the value of threshold is higher than the hop count, it will give false positive rate (that means it give higher alternative route as a true route). In the simulation, first the value of threshold is set one and then the results of the proposed algorithm are calculated. After that, the value of threshold is set two, and the result is again calculated and so on. The simulation of these scenarios shows that increasing the value of threshold the detection ratio of wormhole shows good result. In figure 5 the experiment is run over 51 nodes and it shows the positive result of wormhole detection. In the scenario the value of threshold is decided seven. The figure 1 shows the true path from source to destination before attack. On 25ms the attacker wormhole is activated and it creates a tunnel. The resultant path after the attack is shown in the figure 2 is shorter than the actual path, so the packet will take that path. For detection of wormhole attack in that path, the algorithm run to find an alternative path to the two hop neighbor node. If the hop count of that path is greater than the threshold this path will consider as a wormhole path. the path is S->1->2->3->4->5->6->7->8->9->D. After 25 ms the wormhole nodes that reside in the network perform attack and give the shortest path to the source node, because it is the properties of wormhole that it gives the shortest path to the source by providing the tunnel between two nodes in the path. So after the attack on that path the source node take another shortest path that have wormhole is S->1->2->8->9->D. In this path the source node assume that this is the shortest path and legal path between source and destination. The figure 2 shows that the wormhole node make tunnel between the node 2 and node 8, but the AODV could not detect the tunnel. It is clarify that the proposed technique is detect wither shortest path given by AODV having wormhole or not and it will help network administrator for taking the decision wither selected path is legal or not. From the above consideration of threshold, simulation of proposed technique is compared with the existing AODV. From the analysis we see that the overhead of our technique is more compared to the existing AODV as show in figure 9. A graph of control packet is also shown, because the number of control packets in the proposed technique has increased. In the figure 10, it is shown that when the number of nodes increases the routing load is also increases.

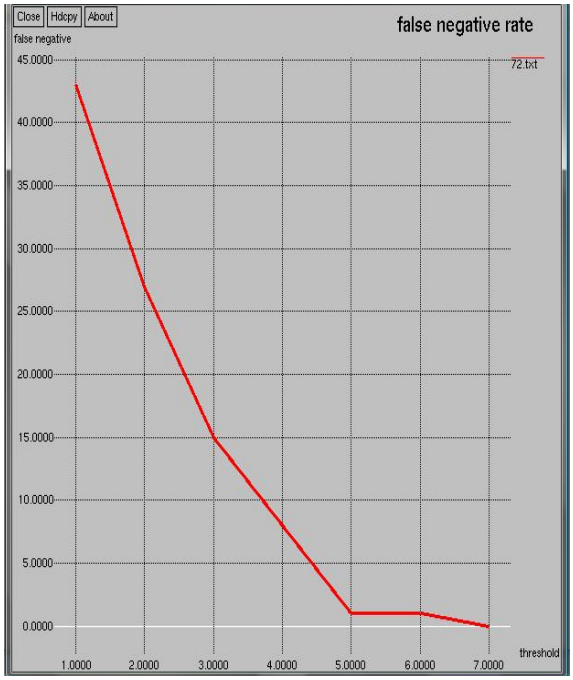

Figure 5 Shows the False Negative vs. Threshold Value for 51 Nodes

In the second scenario the simulation will be done with 72 nodes with same assumptions. We also take the same threshold values for detecting, the false negative result and for a perfect threshold value. After that, we take same scenario with 84 nodes and 100 nodes and result is shown in the figure 7, figure 8.

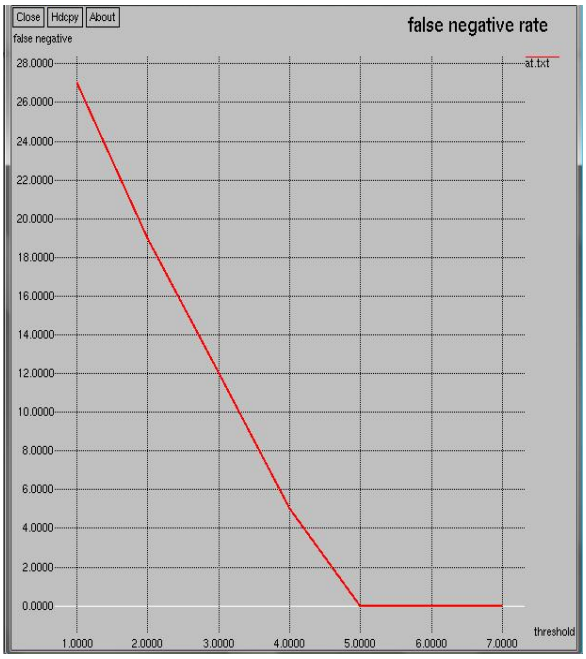

Figure 6 Shows the False Negative vs. Threshold Value for 72 Nodes

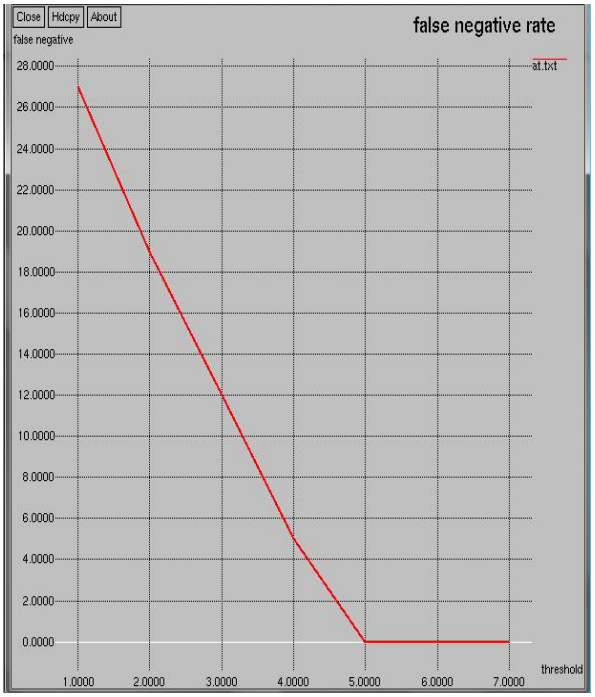

Figure 7 Shows the False Negative vs. Threshold Value for 84 Nodes

Figure 8 Shows the False Negative vs. Threshold Value for 100 Nodes

After the simulation result it can be observed that the actual result is fully depends on threshold value. Result of simulation shows that when the nodes in the network are increased, for detection of a true wormhole, is more compared to the existing AODV. Figure 10 shows the result of control packet and it shows that when the number of nodes increases the value of control packet also increases.

Figure 9 Shows the Result of Routing Overhead

Figure 10 Shows the Result of Control Packet

The above observation shows that the detection technique works efficiently but having some overhead, control packet is also increases in the graph, but the benefit of this technique is that it detects the wormhole, and will serve as an advantage when added to the existing AODV protocol.

7. CONCLUSIONS

A simple technique for detecting wormholes in ad hoc networks is presented in the paper. This method employs routing variation between neighbors to determine the existence of a wormhole. The technique is localized, requires only a small overhead, and does not have special requirements such as location information, accurate synchronization between nodes, special hardware. The technique was tested through simulations for different distributions of nodes and wormholes and different connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent detection probabilities with few false alarms that depend on the value of threshold. Future work includes developing a technique for removal of the wormhole when detected.

8. REFERENCES

[1] "Wireless Networks," wikipedia.org, [Online] Available: network [Accessed: nov, 2012].

[2] Xiangyang Li "Wireless Ad Hoc and Sensor Networks: Theory and Applications" Cambridge University Press 978-0-521-86523-4

[3] Katrin Hoeper, Guang Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," Signals and Communication Technology, pp. 65-82, 2007.

[4] Kanika Lakhani, Himani bathla, Rajesh Yadav "A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET" IJCSNS International Journal of Computer Science and Network Security, vol. 10 No.5, May 2010.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in Proc. of IEEE ICNP, 2002.

[6] Sang-min Lee, Keecheon Kim "An Effective Path Recovery Mechanism for AODV Using Candidate Node" springerlink, vol. 4331/2006, 2006.

[7] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proc. of IEEE INFOCOM, 2003.

[8] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in Proc. of IEEE INFOCOM, 2007.

[9] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks," Computer Network, vol. 51, no. 13, pp. 3750–3772, 2007.

[10] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks: Research articles," Wireless Communication Mobile Computing, vol. 6, no. 4, pp. 483–503, 2006.

[11] X. Su and R. V. Boppana, "On mitigating in-band wormhole attacks in mobile ad hoc networks," in Proc. of IEEE ICC, 2007.

[12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks"

[13] C. Perkins, E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.