PREVENTING WORMHOLE ATTACK IN WIRELESS AD HOC NETWORKS USING COST-BASED SCHEMES

Marianne Amir Azer
Nile University, Cairo, Egypt

Sherif Mohammed El-Kassas
American University in Cairo,Cairo, Egypt

Mady Saiid El-Soudani
Faculty of Engineering, Cairo University, Egypt

Keywords: Ad Hoc networks, Attacks, Routing, Security, Wormhole attack.

Abstract: Ad hoc networks can be rapidly deployed and reconfigured. Hence, they are very appealing as they can be tailored to lots of applications. Due to their features, they are vulnerable to many attacks. A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad-hoc networks. During the attack a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. In this paper we explain the wormhole attack modes and propose two schemes for the wormhole attack prevention in ad hoc networks. The schemes rely on the idea that usually the wormhole nodes participate in the routing in a repeated way as they attract most of the traffic. Therefore, each node will be assigned a cost depending in its participation in routing. The cost function is chosen to be exponential in powers of two such that to rapidly increase the cost of already used nodes. Besides preventing the wormhole attack, these schemes provide a load balance among nodes to avoid exhausting a node that is always cooperative in routing.

1 INTRODUCTION

A wireless ad-hoc network consists of a collection of autonomous peer mobile nodes that self-configure to form a network and have no pre-determined organization of available links. The broadcast nature of the radio channel introduces characteristics to ad hoc wireless networks that are not present in their wired counterparts. Ad hoc networks are vulnerable to attacks due to many reasons, amongst them are the absence of infrastructure, wireless links between nodes, limited physical Protection, and the Lack of a centralized monitoring or management, and the resource constraints. One of the most famous and dangerous attacks to this type of networks is the wormhole attack. During the attack a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. In this paper we suggest a scheme to prevent this attack.

The remainder of this paper is organized a follows. In section 2, we explain briefly the Ad Hoc on Demand Distance Vector (AODV) protocol used for routing in ad hoc networks, and explain in details the different modes of the wormhole attack. In section 3, a suggested scheme for the wormhole attack prevention using two approaches is presented. Finally, Conclusions and future work are given in section 4.

2 BACKGROUND

In this section we give a brief overview on the AODV routing protocol and explain the wormhole attack in details in sections 2.1 and 2.2 respectively.

Amir Azer M., Mohammed El-Kassas S. and Saiid El-Soudani M. (2009).
PREVENTING WORMHOLE ATTACK IN WIRELESS AD HOC NETWORKS USING COST-BASED SCHEMES.
In *Proceedings of the International Conference on Security and Cryptography*, pages 69-74
DOI: 10.5220/0002178400690074

2.1 The Ad Hoc on Demand Distance Vector Routing Protocol

The AODV (Perkins and Royer, 2000) builds and maintains routes between nodes only as needed by source nodes. When a source node desires a route to a destination for which it does not already have a route it broadcasts a RREQ packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the routing tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware.

A node receiving the RREQ may send a RREP if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ, which they have already processed, they discard it and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained.

A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

2.2 The Wormhole Attack

A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad-hoc networks (Karlof and Wagner, 2003),(Hu et al.,2003), (Hu and Evans, 2004). During the attack (Khalil et al., 2005), a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. This tunnel makes the tunnelled packet arrive either sooner or with less number of hops compared to the packets transmitted over normal multihop routes. This creates the illusion that the two end points of the tunnel are very close to each other. A wormhole tunnel can actually be useful if used for forwarding all the packets. However, it is used by attacking nodes to subvert the correct operation of ad-hoc and sensor network routing protocols. The two malicious end points of the tunnel can then launch a variety of attacks against the data traffic flowing on the wormhole, such as selectively dropping the data packets. The wormhole attack can affect network routing, data aggregation and clustering protocols, and location-based wireless security systems. Finally, it is worth noting that the wormhole attack can be launched even without having access to any cryptographic keys or compromising any legitimate node in the network.

The wormhole attack can be launched in at least five different methods as follows.

Packet encapsulation in which a malicious node at one part of the network hears the RREQ packet. It tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the RREQ. The neighbors of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multihop paths. This prevents nodes from discovering legitimate paths that are more than two hops away.

Use of an out of band channel, this channel can be achieved, for example, by using a long-range directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability.

Use of high power transmission, in this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination even without the participation of a colluding node. *Use of packet relay* is another mode of the wormhole attack in which a malicious node relays packets between two distant nodes to convince them that they are neighbors. It can be launched by even one malicious

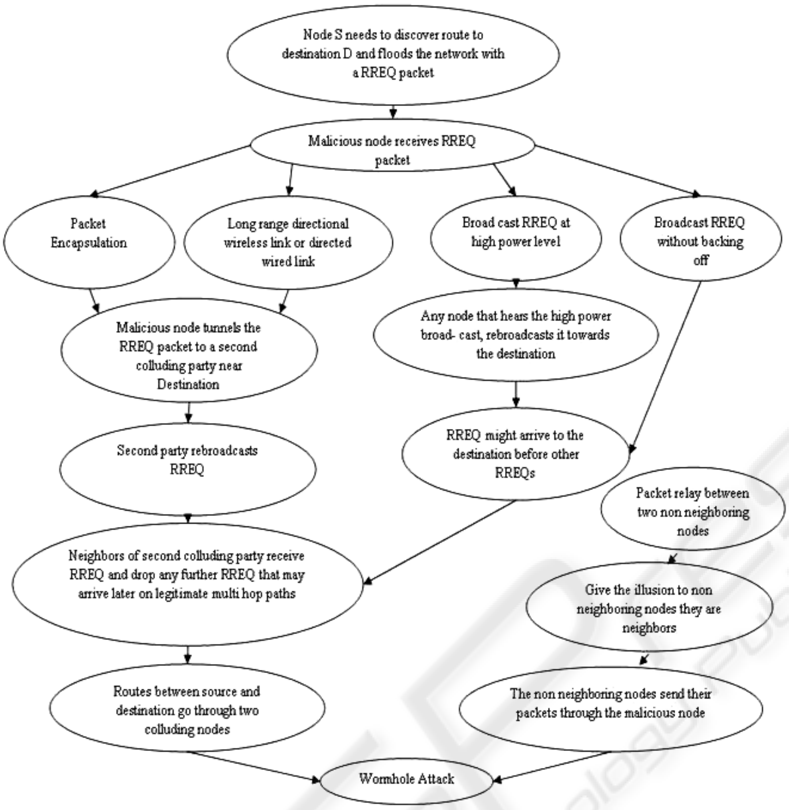
Node S needs to discover route to destination D and floods the network with a RREQ packet
Malicious node receives RREQ packet
Packet Encapsulation
Long range directional wireless link or directed wired link
Broad cast RREQ at high power level
Broadcast RREQ without backing off
Malicious node tunnels the RREQ packet to a second colluding party near Destination
Any node that hears the high power broad- cast, rebroadcasts it towards the destination
Second party rebroadcasts RREQ
RREQ might arrive to the destination before other RREQs
Packet relay between two non neighboring nodes
Neighbors of second colluding party receive RREQ and drop any further RREQ that may arrive later on legitimate multi hop paths
Give the illusion to non neighboring nodes they are neighbors
Routes between source and destination go through two colluding nodes
The non neighboring nodes send their packets through the malicious node
Wormhole Attack

Figure 1: Attack graph of the wormhole attack.

ode. Cooperation by a greater number of malicious nodes serves to expand the neighbor list of a victim node to several hops.

Protocol deviation, during the RREQ forwarding, the nodes typically back off for a random amount of time before forwarding reduce MAC layer collisions. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination.

We have developed an attack graph that depicts the different modes of the wormhole attack, it is depicted in Figure 1.

3 WORMHOLE ATTACK PREVENTION SCHEME

The basic idea that lies behind the wormhole attack is that the wormhole malicious nodes pull the traffic by advertizing short paths, with minimum number of hops. It is therefore more likely possible to have those wormhole routes participate in routing packets. From this perspective, we suggest to modify the AODV protocol in such a way to disable the malicious nodes to attract the traffic all the time and be able to process it maliciously. Hence, each node will be assigned a cost using the cost function in the equation below.

$$c(i)_{new} = 2^n + c(i)_{old}$$

where

$c(i)$ is the cost of a node i

n is the number of times a node has contributed in routing to a certain destination, initially $n = 0$.

This function takes into consideration the number of times a node has participated in routing for a certain source and the node's cost will be increased accordingly.

Two approaches are suggested for dealing with the node's cost. The first is called cumulative cost calculation, and the second is called adaptive step by step cost calculation, these solutions will be presented in sections 03.1 and 3.2 respectively.

3.1 Cumulative Prevention Method

In order to apply our approach three additional features should be added /modified in the default

AoDv protocol. One concerns the RREQs, the other concerns the RREPs and the added cost function. To start with, it was mentioned earlier in the default AODV protocol description that if a node receives a RREQ, which it has already processed, it discards the RREQ and does not forward it. This step should be modified as we need to have multiple options of routing paths for the same request originated by the source. It follows that a node should process all arrived RREQs forwarded to it by different previous hops. In addition, it was also mentioned in the default AODV protocol that as the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. This means that the RREP contains only a pointer to the past hop that forwarded it. To be able to apply our suggested scheme, an extra field that stores the hop list contributing in the path should be added to the RREP packet.

Now if a source node needs a route to the destination, it broadcasts the RREQ packets, which will be now processed differently at intermediate nodes, as described above. When the source node receives the RREP packets, it retrieves the hop names from the extra added field, calculates each path's cost and chooses the path with the minimum cost. A node that has been used more than once has its cost increased exponentially (power of two), this is to ensure that a "tempting" path that offers apparently small number of hops will have a high cost because it contains a node that was used before. By this the "attractive wormhole node" will not be able to attract the traffic as there cost will increase very fastly. To illustrate the idea of path selection at the source node, let us consider the following example:

If a source node has received multiple RREPs for different RREQs that it has sent and a different times starting from t_1 (oldest) to t_n (most recent), i.e

At t_1: only one RREP_a was received after the broadcasting of RREQ_a and the hops' list retrieved from this RREP_a is $\{n_2, n_5, n_7\}$, where n_i is the node id

At $t_{2,}$ another RREQ_b was broadcasted to may be another destination, a RREP_b was received and the list retrieved from this RREP_b is: $\{n_1, n_2, n_{4,} n_6\}$,

At t_3, another RREQ_c was broadcasted to may be another destination, a RREP_c was received and the list retrieved from this RREP_c is: $\{n_3, n_5, n_8\}$,

If at t_4 another RREQ_d was broadcasted to may be another destination, Two RREPs, $\text{RREP}_{d,1}$ and and $\text{RREP}_{d,2}$ were received. The lists retrieved from these RREPs are: $\{n_2, n_{4,}, n_{6,} n_7\}$, and $\{n_1, n_3, n_5\}$.

Where the subscripts *a,b,c,d* denote an ID associated with the RREQs and RREPs. The cost tables are kept and updated at Source, according to Table 1. From Table 1, it is clear that when there is no other alternative for routing the proposed route is selected. However, at time t_4 the path with minimum cost was selected, avoiding as much as possible intermediate nodes repetition. If by coincidence some paths have equal minimum cost, the path with minimum number of hops will be selected.

Table 1: Cost tables at source.

time	**List of available routes**	**Node** Cost **C(*i*), initially=2^0**	**Path Cost**
t_1	$\{n_2, n_5, n_7\}$	C(2)=1 C(5)=1 C(7)=1	3
t_2	$\{n_1, n_2, n_{4,} n_6\}$,	C(1)=1 C(2)=3 C(4)=1 C(6)=1	6
t_3	$\{n_3, n_5, n_8\}$,	C(3)=1 C(5)=3 C(8)=1	5
t_4	$P_1=\{n_2, n_{4,}, n_{6,} n_7\}$	C(2)=7 C(4)=3 C(6)=3 C(7)=3	16
	$P_2=\{n_2, n_3, n_5\}$	C(2)=7 C(3)=3 C(5)=7	17

3.2 Adaptive Step by Step Prevention Method

Another approach using the same suggested cost function makes a hop based decision. The following algorithm and the flow chart shown in Figure 1 describe this hop-based decision.

1-A signaling packet (RREQ/RREP) is received by node (X) from Node (N).

2-Node (X) extracts target Source or Destination (S/D) from signaling packet (If the signaling packet is a RREQ then the target is the source, if the signaling packet is a RREP, then the target is the Destination).

3-Node (X) searches in routing table for another node (O) having a fresh route to the target

4-If the node (O) is not found or if the route is not fresh enough, node (N) is added to the routing table of node (X).

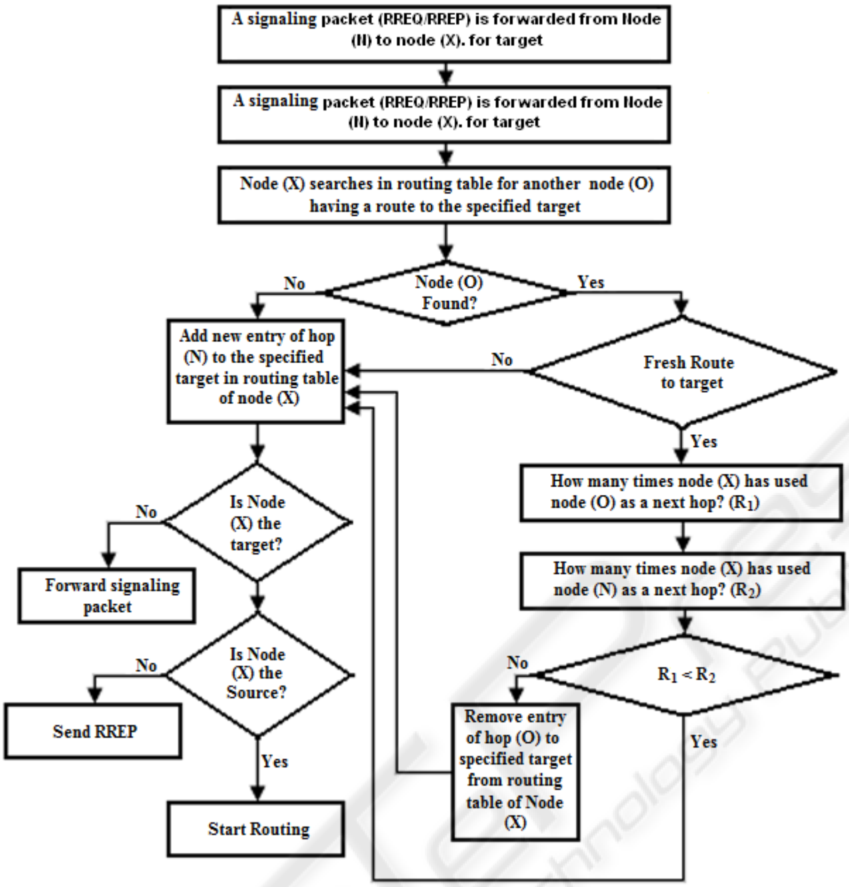
A signaling packet (RREQ/RREP) is forwarded from Node (N) to node (X). for target
A signaling packet (RREQ/RREP) is forwarded from Node (N) to node (X). for target
Node (X) searches in routing table for another node (O) having a route to the specified target
Node (O) Found?
No
Yes
Add new entry of hop (N) to the specified target in routing table of node (X)
Fresh Route to target
No
Yes
How many times node (X) has used node (O) as a next hop? (R1)
How many times node (X) has used node (N) as a next hop? (R2)
Is Node (X) the target?
No
Forward signaling packet
Is Node (X) the Source?
No
Send RREP
Yes
Start Routing
R1 < R2
No
Yes
Remove entry of hop (O) to specified target from routing table of Node (X)

Figure 2: Flow chart of adaptive step by step wormhole attack prevention.

5-If the node (O) is found in the routing table, and has a route to the target the following should be verified:

i- How many times node (X) has used node (O) as a next hop (R_1)?

ii-How many times node (X) has used node (N) as a next hop (R_2)?

iii- Compare R1 and R2

iv- Update the routing table

4 CONCLUSIONS AND FUTURE WORK

Throughout this paper, we introduced the wormhole attack and the effort that has been done in the literature either to prevent, or to detect this attack, we have also explained briefly the AoDV protocol used in the ad hoc networks for routing. A wormhole prevention scheme was suggested. To prevent the wormhole attack, we suggested the modification of the AODV protocol in such a way to disable the malicious nodes from attracting the traffic all the time and be able to process it maliciously. The idea relies basically on assigning cost to the nodes that participate in routing packets for a certain source. A node that has been used more than once to route packets for a certain source has its cost increased exponentially (power of two). Based on this idea, we suggested two wormhole attack prevention schemes. In the first scheme, called cumulative prevention, the source node receives the RREP packets, it retrieves the hop names from the extra added field, calculates each path's cost and chooses the path with the minimum cost. A node that has been used more than once has its cost increased exponentially (power of two), this is to ensure that a tempting path that offers apparently small number of hops will have a high cost because it contains a node that was used before. By this, the attractive wormhole node will not be able to attract the traffic as there cost will increase very fastly. The second solution is an adaptive step by step prevention method and uses the cost function to compare, at every node receiving a control message, between a next hop offering a route to the destination and nodes in its routing table also having routes to the destination. In addition to preventing the wormhole attack, those solutions have the privilege of providing a load balance in the ad hoc networks, such as to save regular nodes from resource consumption if they repeatedly participate in routing. We plan to verify those schemes, while comparing its performance to other wormhole prevention schemes proposed in the literature. In addition, the cost function can include extra calculations to take the number of hops offered by a path into account such as to have the minimum path cost and hop count together.

REFERENCES

Perkins, C., Royer, E., 2000. The Ad hoc On-Demand Distance Vector Protocol. *In C. E. Perkins, editor, Ad hoc Networking, Addison-Wesley, pp. 173-219.*

Karlof C., Wagner,D., 2003.Secure Routing in Sensor Networks: Attacks and Countermeasures. *In the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.*

Hu, Y., Perrig, A., Johnson, D.,2003. Packet leashes: a defense against wormhole attacks in wireless networks. In *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM),* pp. 1976-1986.

Hu, L., Evans, D., 2004. Using Directional Antennas to Prevent Wormhole Attacks, *In Network and Distributed System Security Symposium (NDSS).*

Khalil,I., Bagchi, S., Shroff, N., 2005. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. *In 2005 International Conference on Dependable Systems and Networks (DSN'05),* pp. 612-621.

Choi, S., Kim, D., Lee, D., Jung, J., 2008. WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks. In *Sensor Networks, Ubiquitous and Trustworthy Computing 2008 SUTC '08*. IEEE International Conference on, vol., no., pp.343-348.

Khurana, S., Gupta, N., 2008. FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks. In securware *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, pp.74-79.

Wang, X., 2006. Intrusion Detection Techniques in Wireless Ad Hoc Networks. In *30th Annual International Computer Software and Applications Conference (COMPSAC'06)*, pp. 347-349, 2006.

Wang, X., Wong, J., 2007. An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks. In *31st Annual International Computer Software and Applications Conference - Vol. 1- (COMPSAC 2007)*, pp. 39-48.

Zhang, Y., Liu, W., Lou, W., and Fang, Y, 2005. Securing sensor networks with location-based keys. In *WCNC 2005, IEEE Wireless Communications and Networking Conference, no. 1, pp*. 1909 – 1914.

Poovendran, R., Lazos, L., 2007. A graph theoretic framework for preventing the wormhole attack. In *wireless ad hoc networks, Volume 13, Issue 1,* ISSN: 1022-0038, pp. 27 – 59, 2007.

Song,N., Qian, L., Li, X., 2005. Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach. In *19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 17*.

Buttyan, L., Dora, L., Vajda, I., 2005. Statistical wormhole detection in sensor networks. In Hungary, July 2005.

Maheshwari, r., Gao, J., Das, S., 2007 Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information, In *INFOCOM 2007, 26th IEEE International Conference on Computer Communications, IEEE (2007*), pp. 107-115.

Wang, W., Bhargava, B., 2004. Visulization of wormholes in sensor networks. *In Proceeding of the ACMWorkshop onWireless Security (WiSe)*, pp. 51–60, 2004.

Azer, M., El-Kassas, S., El-Soudani, M., 2006. Using Attack Graphs in Ad Hoc Networks for Intrusion Prediction Correlation and Detection. In *SECRYPT* 2006, pp. 63-68.

Win, K., 2008. Analysis of Detecting Wormhole Attack in Wireless Networks. In *Proceedings of world Academy of Science, Engineering and Technology Volume 36 December 2008 ISSN 2070-3740.*

Kong, F., Li, C., Ding, Q., Cui, G., and Cui, B., 2009. WAPN: A Distributed Wormhole Attack Detection Approach for Wireless Sensor Networks. In Journal of Zhejiang University SCIENCE A, vol. 10, pp. 279~289, February 2009.

Gunhee, L., Jungtaek, S., and Dong-kyoo, K., 2008. An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks," in Proceedings of the 2008 International Conference on Information Security and Assurance (ISA 2008), pp. 220-225.