ROMANIAN JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE, 2013, VOLUME 3, ISSUE 1, p.60-70

RESIST SRP AGAINST WORMHOLE ATTACK

Marjan Kuchaki Rafsanjani*, Mahmoud Eshraghi Samani**

Abstract

Ad-hoc networks refer to temporary or interim networks which form for special purposes. Actually they are wireless networks with mobile nodes. These networks use no network assisting element for path routing and in these networks available nodes are responsible for path routing. Therefore when malicious nodes want to find a way to interfere with the path routing then the existence of a secure route protocol (SRP) can prevent the interference. SRP protocol is one of the secure algorithms of path routing protocol but it is not resistant against wormhole attack. Wormhole attack is considered as a subtle attack in which two malicious nodes make a short connection in network's topology through private or implicit connection and represent two non neighbor nodes as neighbors and prevent the correct operation of path routing protocol by using this method. One of the methods of preventing wormhole attack is by using packet leashes. We try to decrease the wormhole attack occurrence in this routing protocol by a kind of packet leashes called temporal leashes. We also will minimize problems resulting from using temporal leashes by different methods and modifications in its structure.

Mathematics Subject Classification: 68M12.
Keywords: wormhole attack, SRP, secure routing protocol, temporal leash.

1. Introduction

Ad-hoc networks refer to temporary or interim networks which form for special purposes. Actually they are wireless networks with mobile nodes. Major difference of Ad-hoc networks with common wireless 802.11 networks is that in ad-hoc networks there is a collection of wireless mobile nodes without any infrastructure (like central station, router, switch or any other things) which are used in other networks in order to help network's structure [10].

Mobile nodes are equipped with receiver and transmitter for making wireless connections. Mobile nodes cannot make contact with all nodes directly because of some limitations in receiver and transmitter. Therefore it is necessary that data to be transferred through other nodes when there is no direct connection. Mobile nodes caused the network to be constantly changing and different paths to be appeared between two nodes. We can refer to personal applications like connection of laptops together, public applications like communication of vehicles and taxies, military

**Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran, E-mail: kuchaki@uk.ac.ir*
***Department of Computer, Science and Research Branch, Islamic Azad University of Kerman, Kerman, Iran, E-mail: mahmoudeshraghi@yahoo.com*

applications like military communication of warships, and emergency applications like rescue and relief operations among other application of this network.

In ad hoc networks no network assisting element is used for routing. Nodes are responsible routing in the network. These networks may have various applications due to no using of predetermined infrastructure. These networks can be easily started up, used and finally removed.

The advantage of this network is its speed and easy operation and also it has no dependency on predetermined infrastructures.

So only those nodes in the effective range of other nodes can receive each other's message and recognize it from noise environment and each node also both are used as an end-system and as path routing for other nodes in the network [1, 3, 7].

2. Wormhole Attack

One of famous special attacks of MANETs is wormhole attack. During the attack two malicious nodes make a short connection cooperatively in network's topology. Mentioned attacks with following order:

Requesting of routing through one node reaches for one of the malicious nodes .Then malicious node sends this request to second node through one private network or through tunneling. Now if these two nodes do not change hop counter value then a long amount of path has been passed through the private network without increasing hop values. Thus it is possible to get to the destination just with two hopes rather than ten hopes. In this case certainly this path chooses as the shortest path. Therefore both are involved in created path .These two nodes cooperate together and force original node to accept relatively incorrect routing information [2, 6].

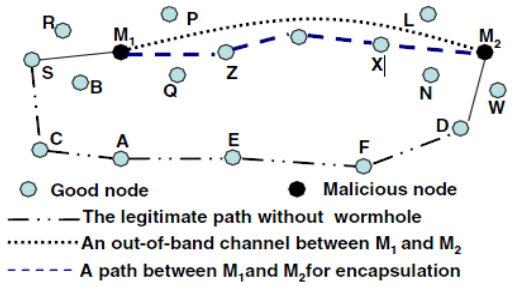

Figure 1. Sample (wormhole attack)

A. Wormhole Attack Effects

It can be demonstrated that if the amount of malicious nodes to be $n>1$ then average amount of $(1-1/n)*100\%$ connections are affected. Also wormhole attack leads to DoS (Denial of Service) with removing of data or removing of control packet. Wormhole attack can lead to gray hole attack or black hole attack and malicious nodes can perform statistical analysis of data flow [5].

3. SRP Protocol (Secure Routing Protocol)

SRP focus on bi-directional communication between a pair of nodes [9]. A security association (SA) between the source node S and the destination node T is assumed. The trust relationship could be instantiated, for example, by the knowledge of the public key of the other communicating end. The two nodes can negotiate a shared secret key, e.g., via the Elliptic Curve Diffie-Hellman algorithm, and then, using the SA, verify that the principal that participated in the exchange was indeed the trusted node. For the rest of the discussion, we assume the existence of a shared key $K_{S,T}$. The SA is bi-directional in that the shared key can be used for control (data) traffic flow in both directions. Relevant state has to be maintained in each direction though.

The existence of the SA is justified, because the end hosts chose to employ a secure communication scheme and, consequently, should be able to authenticate each other. For example, such a group (pair) of nodes could have performed a secure key exchange, or an initial distribution of credentials. However, the existence of SA's with any of the intermediate nodes is unnecessary. Finally, it is required that end nodes are able to use static or non-volatile memory.

The adversarial nodes may attempt to compromise the network operation by exhibiting arbitrary, Byzantine behavior. They are able to corrupt, replay, and fabricate routing packets. They may attempt to misroute them in any possible manner and, in general, they cannot be expected to properly execute the routing protocol. Although a set of malicious nodes may mount attacks against the protocol concurrently, we assume that nodes are not capable of colluding within one step of the protocol execution; that is, within the period of broadcasting one query and reception of the corresponding replies. For clarification, we discuss below an attack mounted by two colluding nodes during a single route discovery.

The underlying data link layer (e.g., IEEE 802.11) provides reliable transmission on a link basis, without any requirement of data link security services, such as the Wired Equivalent Protocol (WEP) function. Moreover, links are assumed to be bi-directional, a requirement fulfilled by most of the proposed medium access control protocols, especially the ones employing the RTS/CTS dialogue. It is also expected that a one-to-one mapping between Medium Access Control and IP addresses exists. Finally, the broadcast nature of the radio channel mandates that each transmission is received from all neighbors, which are assumed to operate in promiscuous mode.

The source node S initiates the route discovery, by constructing a route request packet identified by a pair of identifiers: a query sequence number and a random query identifier. The source and destination and the unique (with respect to the pair of end nodes) query identifiers are the input for the calculation of the Message

Authentication Code (MAC), along with $K_{S,T}$. In addition, the identities (IP addresses) of the traversed intermediate nodes are accumulated in the route request packet.

Intermediate nodes relay route requests, so that one or more query packets arrive at the destination, and maintain a limited amount of state information regarding the relayed queries, so that previously seen route requests are discarded. Moreover, they provide feedback in the event of a path breakage, and in some cases they may provide route replies.

The route requests reach the destination T, which constructs the route replies; it calculates a MAC covers the route reply contents and returns the packet to the S over the reverse of the route accumulated in the respective request packet. The destination responds to one or more request packets of the same query, so that it provides the source with an as diverse topology picture as possible. The querying node validates the replies and updates its topology view.

As an illustrative example, consider the topology of Figure 2, comprising ten nodes. *S* queries the network to discover one or more routes to T. The nodes *M1* and M2 are two malicious intermediate nodes. We denote the query request as a list $\{Q_{S,T};n1,n2,..,nk\}$, with $Q_{S,T}$ denoting the SRP header for a query searching for T and initiated by S. The *ni, i{1,k},* are the IP addresses of the traversed intermediate nodes and *n1=S, nk=T*. Similarly, the route reply is denoted as $\{R_{S,T};n1,n2,..,nk\}$. We now consider a number of scenarios of possible security attacks by the two malicious nodes.

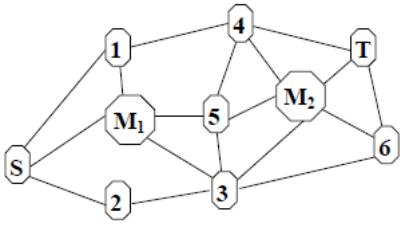

Figure 2. Example Topology: *S* wishes to discover a route to *T* in the presence of two malicious nodes, *M1* and *M2* [9]

Scenario 1: Consider the case that when *M1* receives $\{Q_{S,T};S\}$, it attempts to mislead *S* by generating $\{R_{S,T};S,M1,T\}$. Not only would S accept such a reply, if a regular routing protocol were used, but it would most probably choose this fake route, since *{S,M1,T}* would have fewer hops than any other legitimate reply. It would also be received with the least delay, because of the close distance between *M1* and *S*. The requirement that the request reaches the destination disallows any intermediate node to provide a reply in this manner, and, the false reply packet is discarded, since *M1* does not possess $K_{S,T}$ and cannot generate a valid MAC.

Scenario 2: Consider the case in which *M1* discards request packets arriving from its neighbors, excluding the one from node 1. This type of malicious act cannot

be countered, but the controlled flooding of the query packets provides the required robustness. By discarding route request packets, a malicious node partially narrows the topology view of S and, to some extend, impedes the network operation. In essence, the malicious node can always hide its incident links, but at the same time it practically removes itself from *S*'s view. Thus, it cannot inflict harm to data flows originating from *S*, since the routes chosen by *S* would simply exclude *M1*.

Scenario 3: As assumed above, *M1* sees and appropriately relays $\{Q_{S,T};S,1,M1\}$; upon arrival of $\{Q_{S,T};S,1,M1,5,4\}$ at T, the reply is generated and routed over the reverse path. When *M1* receives $\{R_{S,T};S,1,M1,5,4,T\}$, it tampers with its content and relays $\{R_{S,T};S,1,M1,Y,T\}$, with Y being any invented sequence of nodes. *S* readily discards the reply, due to the integrity protection provided by the MAC.

Scenario 4: When *M*2 receives $\{Q_{S,T};S,2,3\}$, it corrupts the accumulated route and relays $\{Q_{S,T};S,X,3,M2\}$ to its neighbors, where *X* is a false, invented IP address (or, any sequence of IP addresses). This request arrives at *T*, which constructs the reply and routes it over $\{T,M2,3,X,S\}$ towards S. When node 3 receives the reply, it cannot forward it any further, since X is not its neighbor, and the reply is dropped.

Scenario 5: In order to consume network resources, *M1* replays route requests, which are discarded by intermediate nodes, since they maintain a list of query identifiers seen in the past. This is achieved by the underlying routing protocol itself, within the limitations imposed by the size of the query table. But queries replayed after a significant period of time, will propagate across the network and arrive at *T*. The query sequence number, used only by the end nodes for the query identification, allows *T* to discard such queries. If the request header were corrupted, the query would also be discarded. Similarly, *T* discards fabricated route requests, since malicious nodes cannot generate valid request MAC.

Scenario 6: Assume that *M1*, after observing a few route requests originating from S, fabricates several queries with the subsequent query identifiers. The goal of this attack is to make intermediate nodes store these identifiers and discard legitimate, future $\{Q_{S,T};n1,\ldots,nj\}$ route requests. The cost of this attack is low (a single route request transmission per identifier) and, with the Time-To-Live (TTL) field of the query packet set to a high value, the affected network area may be significantly larger. The query identifier values used by intermediate nodes implementing SRP are 'unique' and random, unlike the query identification field of existing on demand routing protocols, whose values are a monotonically increasing sequence. Consequently, such an attack cannot practically affect the protocol operation, because of the extremely low probability of predicting the query identifiers.

Scenario 7: Node *M1* attempts to forward $\{Q_{S,T};S,M^*\}$; i.e., it spoofs an IP address. Such an act is possible and at the routing protocol level the query would propagate through the network and reach *T*. Consequently, S would accept $\{R_{S,T};S,M^*,1,4,T\}$ as a route. It is apparent that the connectivity information conveyed by such a reply is correct. Indeed, all that *M1* would achieve is to mask its identity, which in general will be temporary. Thus, the malicious node would not achieve

anything more than its placement on a potential $S \rightarrow T$ route, which would have been possible in the first place, without any IP spoofing.

Scenario 8: Now, let us assume that *M*1 attempts to return a number of replies, each with a different spoofed IP address, namely, *Mi,Mi+1,...Mi+j*, i.e., an "extension" of Scenario 7. This would lead *S* to believe that a multitude of possible routes to *T* exist, although, in reality, all of these routes are controlled by *M1*. As explained in Scenario 1, *M1* is not allowed to generate replies, and thus fabricates ones that contain the spoofed addresses. An alternative way for *M1* to mount this attack would be to relay more than one route requests, placing a different IP address in each of them; *T* would generate the corresponding replies, *M1* would relay them back towards the source, and *S* would have no choice but to accept them. Fortunately, such an attack is successfully countered by our protocol: *M1*'s neighbors relay only one route request, with specific source and target nodes and query identifier. For example, nodes 1, 3 and 5 will relay the first of such queries and drop subsequent packets as previously seen requests, thanks to the broadcast channel. If *M1* modified the query identifier, the forged query would be forwarded, but *T* would detect the alteration, due to the MAC, and drop the request.

The only possible attack against the protocol would be if nodes colluded during the two phases of a single route discovery. In such a case, they would manage to make the source node to accept partial false routing information. For example, in Figure1, when *M1* receives the route request, it can tunnel it to *M2*; i.e. discover a route to *M2* and send the request encapsulated in a data packet. Then, *M2* broadcasts a request with the route segment between *M1* and *M2* falsified, e.g. $\{Q_{S,T};S,M1,Z,M2\}$. *T* receives the request and constructs a reply, which is routed over *{T,M2,Z,M1,S}*. *M2* receives the reply and tunnels it back to *M1*, which, then, returns it to *S*. As a result, the connectivity information is only partially correct (in this example, only the first and last link). However, one pair of colluding nodes can convince *S* of only a single false path that will include the two nodes. The reason is that *M2* cannot forward a number of requests towards *T* using spoofed IP addresses, as explained above. Special care is needed for a case similar to Figure 2, where *M2* is adjacent to *T*, with countermeasures discussed in the sequel.

Now let us see what would happen when *M2* is near or neighbor to *T*. *M1* receives route request packet from its neighbors and wants to send it to *M2*. To do so it can use two methods: Encapsulating the route packet or private network.

In first method it encapsulates the packet route request and will send it as data to *M2* (It performs the operation through shortest available route which is already discovered) and receives middle nodes of the mentioned packet and sends it according to available route in the packet header. There is no need to record the property of intermediate node inside the packet (Because routing packet is encapsulated as data) and also there is no need for intermediate node to search in the table related to the routing records or making a new entry in this table. Therefore encapsulated routing

packet will reach to the target more quickly than the case of routing packet, receives its *M2*, extracts routing packet and broadcast it.

Nodes which have received this routing packet will remove the routing packets which will be received thereafter. According to *M2* node location near or in neighboring of T so this routing packet will be the only routing packet which is responded by *T*. In optimistic cases it will be one of the rare packets that will be responded by *T*. Therefore the source node S cannot have a proper topology view of the network and will choose a path including two malicious nodes of *M1* and *M2* because of having fewer hopes.

But in the second method *M1* receives routing packet depending on *M1* and sends it through the private network to the *M2*. This private network will be influential if it includes proper speed and be able to send routing packet to *M2* quickly. When *M2* receives routing packet treats in the previously described manner which leads to wormhole attack occurrence. Therefore SRP routing protocol is not resistance against wormhole attack.

4. Decreasing of Wormhole Attacks

Applicable technique is by using a kind of packet leash called temporal leash .This technique influences on limitation of package life's time and according to packages speed influences on passing distance by packages (which equals the maximum amount of optic speed).

To construct a temporal leash, in general, all nodes must have tightly synchronized clocks, such that the maximum difference between any two nodes' clocks is Δ. The value of the parameter Δ must be known by all nodes in the network, and for temporal leashes, generally must be on the order of a few microseconds or even hundreds of nanoseconds. This level of time synchronization can be achieved now with off the shelf hardware based on LORAN-C, WWVB, or GPS. Esoteric hardware such as cesium-beam clocks, rubidium clocks, and hydrogen maser clocks, could also be used in special applications today to provide sufficiently accurate time synchronization for months.

In temporal leashes time of packet sending is t_s and time of package receiving is t_r .Therefore according to speed (maximum speed of light) it can find that whether the package has passed the path more than enough or not. The package will be removed if it has been passed unusual path for 1 hop. If transmitter wants to prevent package sending for paths more than *L* meter long then the *L* value must be more than $L_{min}=c.\ \Delta$.(It is supposed that the speed of light in the air equals light speed in the void). L_{min} is the amount of distance a packet can pass for Δ time [4].

4.1. Temporal leashes analysis

One of the problems of using temporal leashes is the determination of the amount of the path as a limitation for the packet displacement. This limitation leads to absolute omission of all packets from routes longer than this path but allows all shortest paths of packets to pass [8].

For example if we consider distance limitation as L then T and S nodes in the L space are $L>L'$ .Therefore S node never can send any message to the T node because T node removes the packet as it receives the packet according to the limitation from packet leash. On the other hand if there are two nodes of R and S between $M2$ and $M1$ as $L''=d_{SM1}+d_{M1M2}+d_{M2t}<L$ then the packet leash cannot prevent the occurrence of wormhole attack.

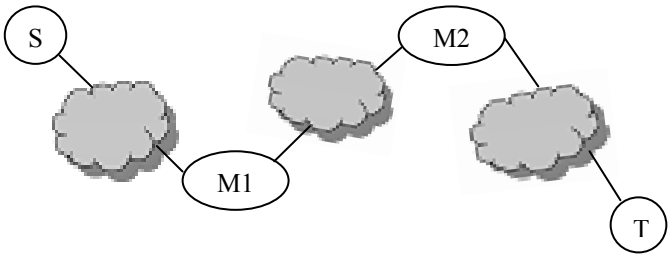

Figure 3. Wormhole prevention

Our purpose is finding a proper value that prevents passing of unauthorized packets. General idea is that a receiver node should calculate the real time for the passing of the package and packet delay in middle nodes in order to find that if the wormhole attack has happened for packet or not. The total amount of delays imposed on the package can be calculated by following formula:

$$D_t=hD_h \qquad (1)$$

in which D_h is delay in one step, h is the number of passed steps by the package. D_h is divided into 3 sections each of which determine delay in one of the layers. Layers of MAC, or Radio ,or network, is influential in path routing but the delay of upper layers has no effect.

On the transmitter node, the timestamp in the network layer placed on the packet's header. Each middle node brings up packet up to the network layer and then sends it again to the lower layer after necessary investigations. Finally receives a packet receiver node and record time after entering network's layer. Calculation of delay values related to each layer is dependent on the algorithm used in it and we use available delay in the layer as used DSR logarithm is different from the available delay value in the layer while we use AODV. The main problem in calculation happens when for example in MAC layer we use 802.11 algorithms. This layer senses media for sending of data and preventing of the collision and it also waits when the occupied value equals n.slot and then sends the package (n is a random number). For removing this problem delay value can be considered based on the kind of network

and our strictness for preventing wormhole attack and the amount of predicted traffic in the network. If the low amount of delay to be considered then it can be assured that no wormhole attack happens. But it is also possible that some admissible packets to be removed. If we consider the high amount of delay then we can assure that no valid packet will be removed but there is a possibility of wormhole attacks and we try to use an average amount of delays.

4.2. To resist SRP against wormhole attack

We use a temporal leash in order to make SRP resistant against wormhole attack .We should make a change in the SRP header in order to SRP be resistant against wormhole attack. We add the time of packet formation in the route request packet. Hereafter we call this time as timestamp and show it with t acronym. We should also use timestamps in calculation of message authentication code (MAC).

We represent the time of a packet arrives to the destination as t_r . Destination node record time as soon as receives a routing request packet in the network layer. D_t Shows the time of in which route request packet has been stopped through the nodes of the network. And we indicate hopes in the whole route as h. When the route request packet reaches its destination the destination node investigates if the relation (2) holds or does not hold; and if the condition is true, then the route reply will be sent.

$$T_r\text{-}t\text{-}D_t \leq ht_h, \qquad (2)$$

where t_h shows required time for sending of the packet one node to the other one. But according to variable distance between nodes we can put average time or maximum required time instead of t_h in order to send the packet from one node to the other one if replace required time average, i.e. t_{havg}, with t_h. Possibility of wormhole attack occurrence will decrease to a large amount which gives following relation :

$$T_r\text{-}t\text{-}D_t \leq ht_{avg}.$$

According to this relation this relation the removal possibility of permissible routing packets will be destroyed. That with increasing of nodes in ad hoc network the possibility of the removing of permissible packets will be much less.

Instead of t_h we can put the maximum required time to send packages from one node to another node (i.e. t_{hmax}) and following relation will be obtained:

$$T_r\text{-}t\text{-}D_t \leq ht_{max}.$$

According to this formula the possibility of the removing of permissible routing packets will be eliminated. But it is possible that wormhole attack happens.

D_t also will be calculated as follows:

$$D_t = t_{mac} + [(t_{extract} + t_{search} + t_{entry})(h\text{-}1)] , \qquad (3)$$

where t_{mac} determines required time for MAC calculation by using hash function in the source node.

$t_{extract}$ is required time for Q_{ID} extraction in addition to the required time for extraction of source and destination node of the route request packet which is calculated for intermediate nodes .

t_{search} is time search in the property table of route request in intermediate nodes.

t_{entry} is required time for inserting properties of route request in related table of intermediate nodes .

Therefore, the table size is specified and limited .So search time and entry time are computable.

5. Conclusion

As it can be seen according to different values for time distance of nodes it can be considered the possibility of wormhole attack occurrence And also the possibility of permissible routing packet removals may become low or high. Therefore the operation of decreasing the possibility of wormhole attack and increasing of permissible route packet removing of tradeoff type should be performed .But if there is required accuracy for limitations then the wormhole occurrence possibility can be prevented and permissible route packet removing will be minimized.

Acknowledgment. The authors would like to express their thanks to the anonymous referees for their comments and suggestions which improved the paper.

References

1. Argyroudis, P. , O'Mahony, D. , *Secure routing for mobile ad-hoc networks*, IEEE Communications Surveys and Tutorials, vol. 7, no. 3, pp. 2 – 21, 2005.
2. Azer, M. A. , El-Kassas, S. M. , El-Soudani, M. S. , *Immuning Routing Protocols from the Wormhole Attack in Wireless Ad Hoc Networks*, Proceeding of the Conference on Systems and Networks Communications (ICSNC '09), pp. 30-35, 2009.
3. Gupte, S. , Singhal, M. ,*Secure routing in mobile wireless ad hoc networks*, AdHoc Networks, vol. 1, no. 1, pp. 151–174, 2003.
4. Hu, Y. C. , Perrig, A. , Johnson, D. B. , Packet leashes: *A defense against wormhole attacks in wire less networks*, Proceedings of the Twenty Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1976-1986, 2003.
5. Khabbazian, M. , Mercier, H. , Bhargava, V. K. , Severity Analysis and Countermeasures for the Wormhole Attack in Wireless Ad Hoc Networks, IEEE Transactions on Wireless Communications, vol. 8, no. 2, Feb. 2009.

6. Khalil, I. , Bagchi, S. , Shroff, N. B. , *MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks*, *Ad Hoc Networks,* vol. 6, no. 3, pp. 344-362, May 2008.
7. Lundberg, J. , *Routing Security in Ad Hoc Networks*, Tik-110.501 Seminar on Network Security, 2000.
8. Moosapoor, M. , *Design and Evaluate a Light-Weight Secure Routing Algorithm in Ad-Hoc Networks*, Master Of Science, Amirkabir University of Technology, Tehran, 2007.
9. Papadimitratos, P. , Haas, Z.J. , *Secure Routing for Mobile Ad Hoc Networks*, Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002.
10. Pervaiz, M., Cardei, M., Wu, J. , *Routing Security in Ad Hoc Wireless Networks*, in: Network Security, Huang S., MacCallum D., Zhu D. (Eds.), Springer, 2005.

ROMANIAN JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE, 2013, VOLUME 3, ISSUE 1, p.60-70