Rendering Wormhole Attacks Trivial using the Scalability Features of a Geocasting Protocol

Appavoo Paramasiven
University of Mauritius
Réduit
Mauritius

ABSTRACT
A number of attacks exist at the network layer, i.e. against routing protocols. One of the most severe attacks is the wormhole attack, which consists of at least two colluding attackers, located at multi-hops distance, that are connected via some unusual means. The attackers replay messages heard at one side to the other side of the network. When this type of attack remains undetected, nodes have the only ability of communicating with at most two-hops neighbor nodes. The detection mechanisms included cryptographic methods and at times the role of specialized nodes which imply either resource-hungry computations or the battery depletion of certain nodes respectively. In this paper, the study of a scalable geocasting routing protocol reveals the required properties, without any costly attack detection mechanism, that render wormhole attacks trivial in a large ad hoc network.

General Terms
Security, ad hoc network, routing protocol

Keywords
Wormhole, attack, ad hoc, network, scalability, geocasting, security, routing

1. INTRODUCTION

1.1 Routing protocols in MANETs
A number of routing protocols were developed depending on certain contexts. They can be broadly classified as unicast or multicast, static or adaptive, proactive or reactive or hybrid, flat or clustered or hierarchical, source routing and geographical. Route discoveries may based on a number of parameters, for example, signal strength, direction of movement, location of destination… In line with the development of routing protocols, a number of attacks emerged. It is implied that if attacks on wireless ad hoc routing protocols critically impact on the communication of nodes, then as the network tends to become larger, the scalability of such protocols is drastically affected. One of the most severe attacks is known as the wormhole attack.

1.2 Scalability of ad hoc routing protocols
Scalability of a routing protocol is whether an acceptable level of delay is maintained as the ad hoc network grows. This is directly related to the number of messages being exchanged as control messages for (1) establishing new routes, and (2) maintaining existing routes. [1, 2] stated that the size of the update message and the frequency of sending the update must be reduced as far as possible. The maintenance of routes needs to be performed in a localized manner.

The scalability of different routing methods is given in [3]. It was noted that hierarchical routing and reactive schemes are preferred to flat routing and proactive schemes respectively. However, hierarchical routing tends to have specialized nodes whose resources deplete quicker than other nodes of the network.

1.3 Anatomy of the wormhole attack
The wormhole attack is illustrated in figure 1, where the attackers are A_1 and A_2. A_1 tunnels whatever message is heard to A_2, on the other side of the network. The latter then replayed the message to its neighbors. The communication channel between the two colluding attackers may be directed antennas or wire. In cases where route discovery procedures were successful and included the wormhole link A_1A_2, all packets sent can be dropped and thus causing denial of service or major network disruptions.

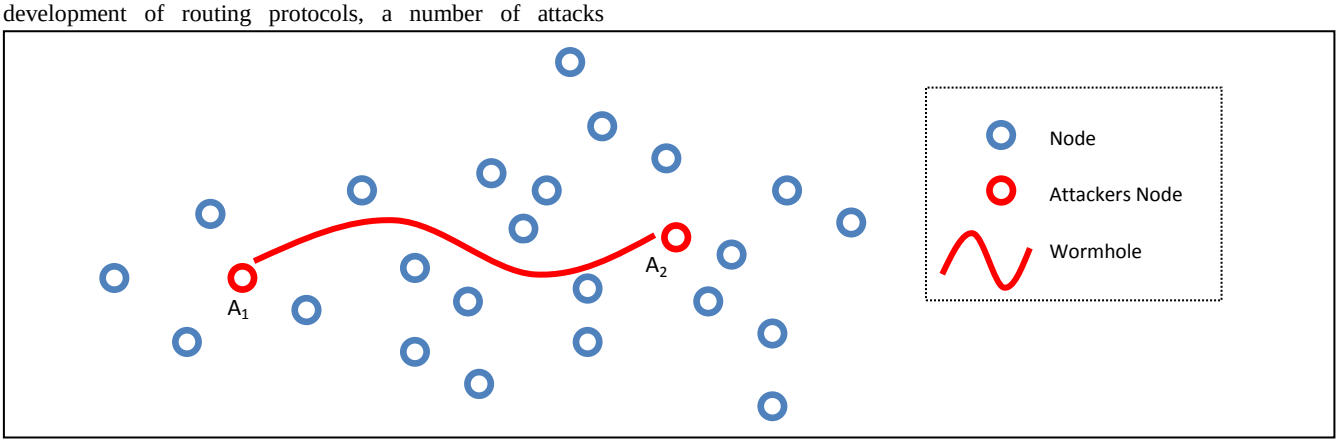

Figure 1. Wormhole attack in ad hoc network

2. RELATED WORK

A number of mechanisms were designed to defend against the different attacks. The most robust one also made use of a proper method of message authentication. The different ways of authenticating messages are (1) Hashing Message Authentication Code (HMAC), (2) Digital signature, and (3) one-way HMAC key chain.

2.1 Methods of message authentication

2.1.1 HMAC – Keyed hashing for message authentication [4]

This method employs a shared key which both the sender and receiver use to verify the message using a one-way hash function. However, intermediate nodes cannot authenticate a message before forwarding. The authentication of messages, given that keys are shared by a pair of node, implies (n*(n-1))/2 to be maintained by each node of the network.

2.1.2 Digital signature [5, 6]

Asymmetric key authentication is preferred as it is not always easy to share a secret key before communicating. The authentication of messages by intermediate nodes implies n keys (n-1 public keys and 1 private key) to be maintained by each node of the network. However, nodes incur unfeasible computations for encrypting and decrypting messages.

2.1.3 One-way HMAC key chain [7, 8]

A key chain of length n is generated by picking randomly picking the first key element, k_0, of the chain and repeated applying a one-way function, F, n - 1 times. Each time F is applied to a key k_i, a new key, k_{i+1}, is generated to form the chain. The keys are then used in the reverse order for authentication. Attackers (1) can compute K_{i+1}, given that k_i was heard and F is known (however, the generated key is considered useless), (2) use k_i, but receiver is expecting the sender to use k_{i-1} as the key for the successive transmission, (3) cannot compute k_{i-1} from k_i.

2.2 Types of routing attacks in ad hoc network

The routing attacks as described in [9, 10, 11, 12, 13, 14] are summarized as shown in table 1.

Table 1: Types of attacks

Attack	Description
Attacks at the data forwarding phase	Nodes alternatively send, drop, modify, replay or flood data packets.
Attacks at the routing maintenance phase	Fake messages requesting for route repairs are broadcasted.
Attacks on route discovery phase	Nodes do not follow the specification of the routing protocol for route discovery. The impact on proactive protocol is more severe than reactive ones as the nodes' resources are depleted in computing non-existent paths. Attacks under this category are further classified as (1) routing table overflow attack and (2) routing cache poisoning attack.
Blackhole attack	The attacker sends fake routing information like acknowledging the availability of a route to a certain destination. Instead of routing data, it simply drops packets in a selective manner so as to avoid neighboring nodes from suspecting its attack.
Byzantine attack	Attacker can operate in solo and inherits the behavior of blackhole attack. It may also work in groups to perform non-optimum data forwarding or in the worst case create routing loops.
Cache poisoning	Using link-state protocols, nodes store the fake information about links to non-neighbor nodes sent by attackers.
Colluding misrelay attack	Attackers work lies on the communication path of sender and receiver. The attacker near the sender forwards the packet, as it is, to the second attacker. This allows the sender to think that the packet is being forwarded in a legitimate manner. However, the second attacker may drop or alter the packet.
Flood rushing attack	This is a rushing attack where a flooded message used the attackers' rushing tunnel to be replayed near the destination. The legitimate flooded message is ignored when it reaches its destination.
Flooding attack	Flood the network with route requests to pointless destination.

Link spoofing attack	Attacker advertises neighbor-relationships with non-neighboring nodes. Neighboring nodes eventually use the attacker node as the multipoint relay to the nodes in the fake advertisement.
Link withholding attack	Attacker does not advertise links to neighbors.
Location disclosure attack	Attacker gathers the locations of nodes so that the network structure can be build to plan attacks.
Resource consumption attack	Attacker depletes nodes' resources by (1) requesting for fake route discovery, and (2) sending data to the victim unnecessarily.
Rushing attack	Quite similar to wormhole, which may result in a denial of service when attackers uses a fast transmission path to replay information request at the destination where the reply is discarded. The request via the genuine path is taken for a duplicate.
Wormhole attack	Attacker replays packets sent at one location to another location. In the event of a route discovery, the shortest path is taken to be the one that was replayed near the destination.

2.3 Preventing wormhole attacks

Two mechanisms [13] were proposed for unveiling wormhole attacks, namely geographical leashes and temporal Leashes, where a leash is the additional information required to limit the packet's travel distance.

With geographical leashes, the additional information required is the location of sender and the time the message was sent. Then the distance that a message is allowed to travel is based on the distance between the receiving node and the sender node in addition to the time taken with respect to the velocity at which the message travels. It also includes a margin for (1) time drift between the concerned nodes, and (2) relative error in the location information. The problem with this method is when two nodes are geographically close but are not within communication range because of obstacles.

With temporal leashes, only the time sent and received are the main determinants for the packet expiration. Each packet contains a time expiration which is an offset from the time sent, which receiving nodes use to compare with their own times respectively. In both cases, a proper authentication mechanism must be present so that an attacker is not allowed to alter the leashes.

In [15], it was proposed that the sending of data is done alternatively along possibly a set of safe routes based on hop counts analysis. It may happen that at times the packets sent may undergone wormhole attack but there is no cost in detecting wormholes. On the other hand, [16] used a local broadcast key, sent by guard nodes, which are used by regular nodes to decrypt the messages from its one-hop neighbor. As such, replayed messages at some other part of the network cannot be consumed by the nodes hearing the message.

3. RENDERING WORMHOLE ATTACKS TRIVIAL

3.1 SENCAST a scalable geocasting protocol

SENCAST, a scalable geocasting protocol [17], was analyzed to show how rushing/wormhole attacks are rendered trivial. SENCAST supports both unicasting and multicasting while bearing scalability features. It is a reactive and geographical protocol.

3.2 Immunity of SENCAST with respect to wormhole attacks

SENCAST establishes route given that (1) IP and location of node are known (unicasting), (2) IP is unknown while location is known (location-based multicast), and, (3) IP is known but location of node is unknown. Given the context information, locations of sender and receiver, the forwarding zone is determined. Only nodes with the forwarding zone will participate as intermediate nodes so that the route initiation message can reach its destination. In case, colluding attackers replays the message, it is very much likely that it will be discarded as the receivers of the replayed message do not lie in the forwarding zone. Intermediate nodes calculate whether they have to forward the packet or not as follows:

Using the location of the source and destination, a node p can derive the equation Y = m(X) + C, where Y and X are the imaginary north/south and east/west lines respectively. Then p needs to finds out the distance between itself and the perpendicular intersection, q, with the imaginary line joining the source, s, and the destination, d. Using the fact that the equation of the line that joins p and q is:

$$\boldsymbol{Y = \frac{-1}{m}(X) + K},$$

and at the intersection:

$$\boldsymbol{Y = m(X) + C = \frac{-1}{m}(X) + K},$$

p derives *q's X* and *Y* coordinates after calculating:

$$\boldsymbol{m = (s.Y - d.Y) \Big/ (s.X - d.X)},$$

$$\boldsymbol{C = s.Y - m(s.X)},$$

$$\boldsymbol{K = p.X + m(p.Y)}$$

If (s.X – d.X) is not equal to 0 and m is not equal to 0, then:

$$\boldsymbol{q.X = \left(\frac{K}{m} - C\right) \Big/ \left(m + \frac{1}{m}\right)},$$

$$\boldsymbol{q.Y = m * q.X + C}$$

If (s.X – d.X) is not equal to 0 and m is equal to 0 (horizontal line), then:

q.X = p.X,

q.Y = C

If (s.X – d.X) is equal to 0, m is equal to ∞ (vertical line), then:

q.X = s.X or q.X = d.X

q.Y = p.Y

Finally *p* calculates the distance between *q* and itself, if the distance is less that the specified forwarding zone range and *q's X* or *Y* coordinates lies between the endpoints *source* and *destination*. Then *p* is a forwarder.

SENCAST also sends three route initiation messages that are intended for three different forwarding zones. The latter may be partially overlapped or fully non-overlapped to be more resilient to wormhole attacks. In case one of the routes is compromised with the colluding attackers, there are still two other functional routes. The number of colluding attackers has to be numerous to fully breakdown the communication path between any two nodes. Therefore, separate multi-paths make such attacks unattractive.

The robustness of SENCAST can be further increased when the destination replies along paths that appear safe. This is achieved by comparing the hop counts in the packets that arrived along the respective forwarding zone. Whenever one of the packets travelled a much lower number of hops than the other two, the destination must refrain from acknowledging through the path of that packet. It is highly probable that the packet got through a wormhole link.

3.3 Possible wormhole attacks scenarios

The possible wormhole attacks scenarios are depicted in figure 2. Given that (1) node S is looking for a path to a node D, whose location is known, and (2) an attacker node A1, close to S, has the possibility of having as colluding attackers Aout or AR or AM or AL for the wormhole, then the following possible scenarios are viable:

Replayed messages from Aout are discarded by receivers as they fall outside the forwarding zones. Therefore when one of the colluding attackers is outside the forwarding zone, there is no impact on the routing protocol.

When both colluding attackers lie within the forwarding zones (A1AR or A1AM or A1AL), they can possibly impact on the proper functioning of the network as the one of the route initiation message reaches the destination, node D, via a wormhole. Node D receives a number of route initiation requests via a number of possible paths across a number of partially-overlapping forwarding zones. However, D replies against paths based on average number of hops the route initiation packets have taken respectively. Safer routes imply neglecting paths where the number of hops are abnormally lower than the computed average.

In case that one of the paths fell under a wormhole attack, the multi-paths routes created across the different forwarding zones respectively increases the resiliency of the network against such attacks.

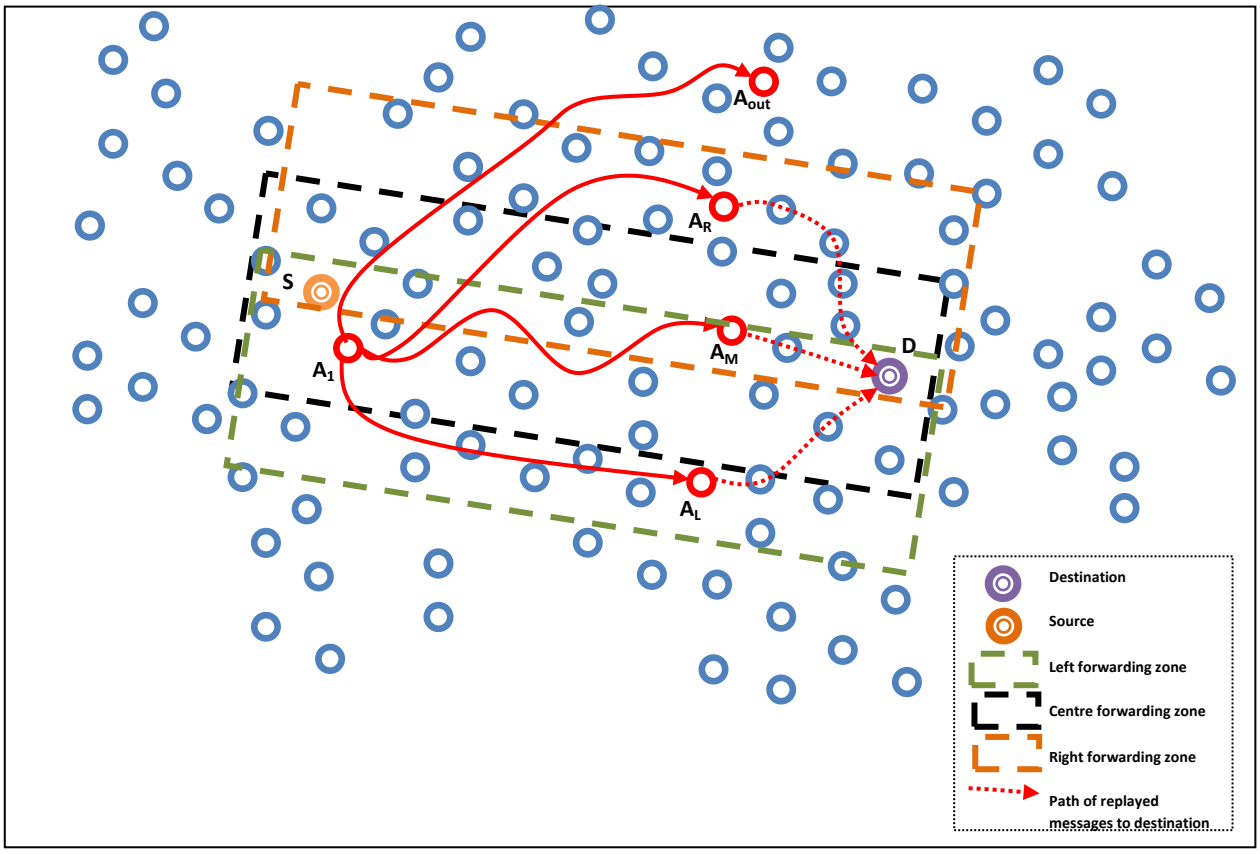

Figure 2. Wormhole attacks' scenarios

The tampering of packets' headers and payloads still represent a severe loophole. The use of one-way key chain is solicited along with a hash function to compute a message digest. This allows the authentication of messages provided that a proper synchronization mechanism is set up for the proper use of key k_i, when not all nodes have been receiving the message that required the key k_{i+1} for prior authentication.

4. CONCLUSION

Wormhole attacks are considered to be among most severe attacks towards the routing protocols of ad hoc network. It has been shown that the properties of a scalable geocasting protocol render such attack as trivial. Without any expensive detection mechanism, nodes can still communicate with other nodes located at multi-hops distance. The points to be noted are (1) the location of receiver and the sender delimits the forwarding zone, therefore replayed messages outside this zone have no effect, (2) a number of route requests is received by the destination, the choice of the route reply is on one of the safer routes, based on the number of hops closest to the average, and (3) the use of multipaths spread across a number of non-overlapping zones or partially overlapping zones increases the resiliency against wormhole attack. There are no costs associated with a detection mechanism and the robustness of a protocol can be enhanced with the proper means of message authentication.

5. REFERENCES

[1] A. Iwata, C. Chiang, G. Pei, M. Gerla and T. Chen 1999. Scalable routing strategies for ad hoc wireless networks. IEEE Journal on Selected Areas in Communications SAC. Vol. 17, pp. 1369-1379.

[2] G. Pei, M. Gerla and T. Chen 2000. Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks. IEEE International Conference on Communications. Vol 1, pp. 70-74.

[3] X. Hong, K.Xu and M. Gerla, 2002, Scalable routing protocols for mobile ad hoc networks. IEEE Network. Vol 16, pp. 11-21.

[4] Mihir Bellare, Ran Canetti and Hugo Krawczyk 1996. Keying Hash Functions for Message Authentication. Advances in Cryptology - Crypto 96 Proceedings. Lecture Notes in Computer Science Vol. 1109. N. Koblitz ed., Springer-Verlag.

[5] R. L. Rivest, A. Shamir, and L. Adleman, MIT Laboratory for Computer Science 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol 2, No. 2.

[6] Taher Elgamal 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory. Vol. IT-31, No. 4.

[7] Yih-Chun Hu, Adrian Perrig and David B. Johnson 2002. Ariadne: A Secure On-Demand RoutingProtocol for Ad Hoc Networks. MobiCom'02 Conference.

[8] Yih-Chun Hu, David B. Johnson and Adrian Perrig 2003. SEAD: Secure Efficient Distance Vector Routing for MobileWireless Ad Hoc Networks. Ad Hoc Networks, Elsevier.

[9] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang 2004. Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications.

[10] Y. Xiao, X. Shen, and D.-Z. Du 2006. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless/Mobile network security, Springer.

[11] Rashid Hafeez Khokhar , Md Asri Ngadi and Satria Mandala 2008. A Review of Current Routing Attacks in Mobile Ad Hoc Networks. International Journal of Computer Science and Security. Volume (2) issue (3).

[12] Daniel Raffo 2005. Security schemes for the OLSR protocol for ad hoc networks. PhD thesis, University de Paris 6.

[13] Yih-Chun Hu, Adrian Perrig, and David B. Johnson 2006. Wormhole Attacks in Wireless Networks. IEEE Journal on selected areas in Communications. Vol 24, No. 2, pages 370-380.

[14] Kannhavong B., Nakayama, H., Nemoto Y., Kato N., Jamalipour A. 2007. A survey of routing attacks in mobile ad hoc networks. Pp 85 – 91, Vol 14.

[15] Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo 2009. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. Sensors 2009, 9, 5022-5039.

[16] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang 2005. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. Wireless Communications and Networking Conference IEEE. Pp 1193 - 1199 Vol. 2.

[17] P. Appavoo and K. Khedo 2008. SENCAST: A Scalable Protocol for Unicasting and Multicasting in Large Ad hoc Emergency Network. Vol.8 no.2 pp 154-165, IJCSNS.