ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Analysis of Secured Energy Efficient Key Management in Wormhole Attack

M.Mythily, S.Saravana Kumar
Research scholars, Dept of Computer Science Engineering, Bharath University, Chennai, India
Professor, Department of IT, Panimalar Institute of Technology, Chennai, India

ABSTRACT: The ad-hoc networks are the temporarily established wireless networks which does not require fixed infrastructure it is also called as infrastructure less network. Because of some flaws of ad-hoc network such as shared wireless medium and lack of any central coordination makes them more prone to attacks in comparison with the wired network. Among all the attacks wormhole attack is the most severe attack. In this attack an attacker capture the packets at one location in the network and send it two another attacker at a distant location through tunnels which is established through different ways like packet encapsulation, using high power transmission or by using direct antennas. This tunnel between two colluding attackers is virtual and it is called as a wormhole. The wormhole attack is possible even if the attacker has not comprised any hosts, and all communication provides authenticity and confidentiality. By using the various approaches for finding the solution over wormhole attack, the dynamic information of the packets could still be modified. So in order to give more robust protection in some special scenario like battlefields, which requires highly secured information? there is need of developing some secured mechanism for wormhole detection. Taking into consideration this problem the proposed scheme is developed. This paper discusses proposed works on wormhole attack along with comparison of different wormhole detection techniques in ad-hoc wireless network.
Keywords: wormhole, attack, wireless, host, packet, wireless.

I .INTRODUCTION

The methods proposed in the previous researches can be broadly classified in to two categories. First, methods which has modified a well known routing protocols such as Ad hoc on Demand Distance vector, Dynamic Source routing, Optimized Link Sate routing to avoid/detect wormhole attack during route request. Second, methods which has adopted an extra hardware or monitoring system such as positioning system, a time synchronization mechanism, directed antenna or intrusion detection system .

II. TECHNIQUES TO REMOVE WORM HOLE ATTACK

2.1 PACKET LEASHES ALGORITHM

To construct a geographical leash[2], in general, each node must know its own location, and all nodes must have loosely synchronized clocks. When sending a packet, the sending node includes in the packet its own location Ps , and the time at which it sent the packet ts; when receiving a packet, the receiving node compares these values to its own location Pr , and the time at which it received the packet tr . If the clocks of the sender and receiver are synchronized to within (+-delta), and v is an upper bound on the velocity of any node, then the receiver can compute an upper bound on the distance between the sender and itself dsr . Specifically, based on the timestamp ts in the packet, the local receive time tr , the maximum relative error in location information , and the locations of the receiver pr and the sender ps ,dsr then can be bounded by .Astandard digital signature scheme or other authentication technique can be used to enable a receiver to authenticate the location an timestamp in the received packet [IEEE 2006].

Two types of packet leash [3,16,17,18] information was used Geographical Leash and Temporal Leash.

In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through a wormhole or not.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

In Temporal Leashes, all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information. When temporal leashes are used, the sending node append the time of transmission to each sent packet *ts* in a packet leash, and the receiving node uses its own packet reception time *tr* for verification. The sending node calculates an expiration time *te* after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from travelling farther than distance L, the expiration time is set to:

$te = ts + (L/c) - \Delta$

Where *c* is the speed of light and Δ is the maximum clock synchronization error. All sending nodes append the time of transmission to each sent packet. The receiver compares the time to its locally maintained time and assuming that the transmission propagation speed is equal to the speed of light, computes the distance to the sender. The receiver is thus able to detect, whether the packet has travelled on additional number of hops before reaching the receiver. Both types ofleashes require that all nodes can obtain an authenticated symmetric key of every other node in the network. These keys enable a receiver to authenticate the location and time information in a received packet.

2.2 BOUNDARY STATE ROUTING (BSR)

BSR is a geographic routing protocol which routes the data using the location of the nodes. In this paper [1] we present the possible attacks on BSR protocol. These attacks are difficult to be detected. To avoid the attacks on BSR protocol, we propose two schemes namely Reverse Routing Scheme (RRS) and Authentication of Nodes Scheme (ANS).

To detect and thus defend against wormhole attacks. In this attack, an attacker records a packet or individual bits from a packet, at one location in the network, tunnels the packet (possibly selectively) to another location, and replays it there.

Geographic routing protocols use a basic geographic forwarding strategy to forward packets node by node toward the location of the destination. This approach to routing has the advantage of eliminating the need for nodes to maintain conventional routing information.

The routing protocol must deal with threats from external agents and compromised internal nodes. The lack of a central control and the fact that each node must forward packets of other nodes represent major security challenges. In such environments it is difficult to assure the confidentiality and the integrity of the communications as well as the availability of the services.

Reverse Routing Scheme (RRS)

In RRS, the destination node tries to reach the source node in the reverse path. The reverse path is not the reverse of the path through the data is traversed from source to destination. Here the destination node sends an acknowledgement called data acknowledge, for the data it has received, to the source node. The acknowledgement packet is sent to the neighbour node that is closer to Source and it is forwarded to the next nodes in reverse greedy forwarding method.

Authentication of Nodes Scheme (ANS)

In ANS type of attack, shown in is detected using this scheme. The attack as mentioned cannot be detected by ordinary methods as the intruders move to the locations such that the traffic is automatically diverted towards them. To avoid this type of attack, verification of authentication details of the nodes in the route is done at the destination node. Here it is assumed that the nodes in the network share their certificates and digital signatures.

In the data packet that is routed through the intermediate node, the node adds its digital signature. All the intermediate nodes must add their digital signatures in the data packet that travelled through it. The signatures are verified at the destination node. If any node without digital signature or false digital signature is found in the data packet, the data packet is taken as untrusty packet and a request is sent to the source node from destination node for the repetition of the packet excluding the nodes that are found to be conspirators, in the new route.

2.3 DELPHI METHOD

Chiu et al. introduce a Method called delay analysis approach [4] which is also called DELPHI. It calculates mean delay per hop of every possible route. DELPHI applied a multi-path approach, and recorded the delay and hop counts in transmitting RREQ and RREP through the paths. After collecting all response, the sender computes mean delay per hop of each route. The path with wormhole attacks, the delay would be obviously longer than a normal path with the same

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

hop count hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided.

2.4 WARP METHOD

Su et al proposed a modified AODV routing protocol [5] called WARP to defend against wormhole nodes by adopting link disjoint multi-path routing between source and destination. In WARP each node records all of its neighbours anomaly values (number of times it forms path from different source to destination). Due to wormhole node's great ability to grab routing paths, if the occurrence of one links exceeds the threshold value, the two ends of this link may be wormhole nodes. If anomaly values of a node exceed a threshold value then its neighbour will discard all requests for forming route containing that node in the path.

2.5 TIME OF FLIGHT TECHNIQUE

Another set of wormhole prevention techniques is similar to temporal packet leashes in [3], is based on the time of flight of individual packets. One possible way to prevent wormholes, as used by Capkun et al in [7] is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range. Another set of wormhole prevention techniques is similar to temporal packet leashes in [6], is based on the time of flight of individual packets. One possible way to prevent wormholes, as used by Capkun et al in [9] is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range. The basis of all these approaches is the following. The Round Trip Travel Time (RTT) δ of a message in a wireless medium can, theoretically, be related to the distance *d* between nodes, assuming that the wireless signal travels with a speed oflight *c*:

$$te = ts + (L/c) - \Delta \quad (1)$$

$$d = \delta * c/2 \quad (2)$$

$$\delta = 2d/c \quad (3)$$

The neighbour status of nodes is verified if *d* is within the radio transmission range *R*:

R > *d* (*d* within transmission range)

$$R > \delta * c/2 \quad (4)$$

$$\delta < 2R/c \quad (5)$$

In essence, the use of RTT eliminates the need for tight clock synchronization required in temporal leashes: a node only uses its own clock to measure time. When a de-facto standard of wireless ad hoc networks 802.11 Medium Access Control (MAC) protocol is used, such calculations are downright impossible. 802.11 imposes a short wait time of 10us (SIFS) between the reception of a packet and sending of 802.11 acknowledgement. When 802.11 is used, transmission range *R* is generally about 300 meters. The speed of light *c* is 3×10–8 *m/s*. Then, from equation 4:

$$\delta = 2d/c = 600m/3 \times 10{-}8\ m/s$$

$$= 0.000002s = 2 \times 10\text{-}6 = 2\ us \quad (6)$$

Therefore, the RTT is an order of magnitude smaller than the delay required by the protocol. We could, of course, account for this processing time by modifying formula 4 in the following manner:

$$\delta = 2d/c + S \quad (7)$$

where S is SIFS(Short Inter frame Space). However, note that wormhole attackers are not limited by the rules of the network, and could send their packets without 802.11-imposed delay.

Approaches based on RTT that one node sends a packet to another, the answer should arrive very shortly, ideally within the amount of time a wireless signal would travel between the nodes. If there is a wormhole attacker involved, packets end up World Academy of Science, Engineering and Technology 24 2008423

2.6 LITEWORP

Khalil et al. [8] introduces LITEWORP in which they used the notion of guard node. The guard node can detect the wormhole if one of its neighbour is behaving maliciously. The guard node is a common neighbour of two nodes to

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

detect a legitimate link between them. In a sparse network, however, it is not always possible to find a guard node for a particular link.

2.7 MOBIWORP ALGORITHM

In [9] two algorithms were proposed which will eliminate the wormhole attack faced when the ad-hoc network is in mobility state called MOBIWORP. In this paper there is a special node called Central Authority (CA) which monitors the node locally and if any malicious activity occurs it isolates the node globally.

MOBIWORP uses local monitoring of neighbourhood communication by each node as a primitive. It does not require specialized hardware at the network nodes, but instead relies on a secure central authority (*CA*) for positiontracking of the mobile nodes and keeping track of adversarial behavior by a mobile node. The use of *CA* appears to fly in the face of the holy design grail of completely distributed protocols. However, the *CA* is contacted only in the event of motion and the protocol can continue to operate through periods when the *CA* is unreachable. To improve scalability and availability, the architecture can accommodate a hierarchical *CA* structure with each *CA* responsible for part of the network. The detection in MOBIWORP is of two types – *local detection* and *global detection*. In the former, the adversarial node is detected by the guards in its current neighborhood in a distributed fashion. In the latter, the adversary is detected on a global network scale by the *CA* aggregating reports from guards at multiple locations. The first protocol proposed under MOBIWORP is called the *Selfish Move protocol* (SMP). In SMP, the mobile node can generate, send, and receive its own traffic but cannot forward any traffic. This design arises from the insight that a node can only launch a wormhole attack if it can forward packets. However, SMP may cause the network to be disconnected if a large fraction of the nodes are mobile at the same time. This scenario is expected to occur in only the most mobile networks.

To address this case, we develop a second protocol called Connectivity Aided Protocol with Constant Velocity (CAPCV). This protocol eliminates the aforementioned lack of connectivity problem by allowing the mobile node to also forward packets. However, this protocol comes with some requirement: the node has to file an "approximate flight plan" with the *CA* giving the average velocity between thecurrent and the new position. Note that in the SMP, the node does not need to determine a priori its trajectory from the source to the destination while in the CAP_CV, it does.

MOBIWORP provides a technique that isolates the malicious nodes from the network thereby removing their ability to cause future damage. The isolation is achieved in two phases – locally, whereby the malicious node is removed from the current neighborhood and globally using global information at the *CA* so that a peripatetic mobile node cannot cause unbounded damage in the network. The detection and the isolation process are done judiciously to minimize the possibility of victimizing innocent nodes due to false alarms caused by natural collisions in the wireless medium or deliberate framing by malicious nodes.

2.8 WHOP PROTOCOL:

WHOP (Wormhole Attack Detection Protocol using Hound Packet) [6] , which is based on AODV, can efficiently found wormhole in the network and also the nodes who were making the wormhole.

In WHOP, a hound packet will be send after the route has been discovered using AODV routing protocol, the hound packet will be processed by every node except nodes who were involved in route from source to destination during path set up. The Principal of WHOP is to take the help of others nodes (nodes who were not involved in path) after the path has been discovered to found worm hole in the network. In path discovery, the protocol uses AODV RREQ packet to find the path from source to destination, RREQ packet being broadcasted by all other node except the destination node. Each node replying back RREP to source node must store its identity into RREP packet. After the source node receives RREP packet, it creates packet called Hound Packet, before forwarding this packet source node computes its Message Digest (MD) and signed the MD with own private key and attached this information with hound packet.

WHOP is very secure protocol against any malicious activity being done by node under scan of hound packet. Hidden wormhole attack can not be possible in WHOP because if node hides its identity while forwarding RREQ or RREP, the nodewho receives such packet after it, would discard the packet because it would not find the last hop entry in the packet as its neighbour.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

III.CONCLUSION

In order to give more robust protection in some special scenario, where highly secured information is required there is a need of developing some secured.

The main objectives of this approach are To prevent eavesdropping, avoid packet modification and provide authentication & confidentiality. To reduce the packet overhead.• To minimize computation in this section, a new group based wormhole detection method has been proposed. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack. A number of recent works have been studied before proposing this new methodology. The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers. or extremely accurate clocks, etc. Currently more studies are being done to analyze the performance of the proposed algorithm in presence of multiple attacker node.

REFERENCES

[1] : Wormhole Attacks in Wireless NetworksYih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[2] : IN THE PAPER Detection and Prevention of Layer-3 Wormhole Attacks on Boundary State Routing in Ad hoc Networks. 2010 International Conference on Advances in Computer Engineering

[3] Y.C. Hu A. Perrig and D. B. Johnson.
PACKET LEASHES: A defense against wormhole attacks in wireless ad hoc networks. IEEE INFOCOM, pages 1976–1986, 2003. 612–621, 2005

[4] : H.S. Chiu and K.S. Lui. DELPHI: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on Wireless Pervasive Computing, pages 6–11, January 2006.

.[5] : Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks.
Computer Security, vol.29, March 2010.

[6] : S Dharmaraja and Subrat kar:WHOP: Wormhole Attack Detection Protocol using Hound Packet. 2011 international conferenceon innovation in information technology

[7]. On the Survivability of Routing Protocols in Ad Hoc Wireless Networks,
A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens, Converence onSecurity and Privacy for Emerging Areas Communications, SecureComm 2005, September2005.

[8]. I. Khalil S. Bagchi and N.B. Shroff.
LITEWORP: a lightweightcounter measure for the wormhole attack in multihop wireless networks.International Conference on Dependable Systems and Networks, pages 612–621, 2005.

[9]: Issa Khalil, Saurabh Bagchi & Ness B. Shroff, "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks". http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4198824

[10] *:* A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks
2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies.1

[11] C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002.

[12]: P. Gupta and P.R. Kumar. Capacity of wireless networks. IEEE Transactions on Information Theory, Volume 46, Issue 2, March 2000, doi:10.1109/18.82579.

[13]: Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris, Capacity of Ad Hoc Wireless Networks, in the proceedings of the 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2001.

[14]: Wu S.L., Tseng Y.C., "Wireless Ad Hoc Networking, Auerbach Publications", 2007 ISBN 978-0-8493-9254-2.

[15]: Tomas Krag and Sebastian Büettrich (2004-01-24). "WirelessMesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.

[16] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks," Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2,pp. 370- 380, 2006.

[17] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", in *proceedings of INFOCOM*, 2004.

[18] W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience, "Defending agains Wormhole Attacks in Mobile Ad Hoc Networks," Wireless Communication and Mobile Computing, January 2006.

[19] Kamatchi P., Selvaraj S., Kandaswamy M., "Synthesis, magnetic and electrochemical studies of binuclear copper(II) complexes derived from unsymmetrical polydentate ligands", Polyhedron, ISSN : 0277-5387, 24(8) (2005) PP.900-908.

[20] M.A. Azer S.M. El-Kassas A. Wahab F Magdy S and El-Soundani.
Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme.
In the proceedings of the IEEE international conference on availability, reliability and security, pages 630–646, 2008.

[21] Babu T.A., Joseph N.M., Sharmila V., "Academic dishonesty among undergraduates from private medical schools in India. Are we on the right track?", Medical Teacher, ISSN : 0142-159X, 33(9) (2011) PP.759-761.

[22] G. Lee D. Kim and J. Seo. An approach to mitigate wormhole attack in wireless ad hoc networks.
In the proceedings of the international conference on information security and assurance, pages 220–225, 2008.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

[23] Suresh V., Jaikumar S., Arunachalam G., "Anti diabetic activity of ethanol extract of stem bark of Nyctanthes arbor-tristis linn", Research Journal of Pharmaceutical, Biological and Chemical Sciences, ISSN : 0975-8585, 1(4) (2010) PP.311-317.
[24] Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks. Computer Security, vol. 29, March 2010.
[25] Singamsetty P., Panchumarthy S., "Automatic fuzzy parameter selection in dynamic fuzzy voter for safety critical systems", International Journal of Fuzzy System Applications, ISSN : 1562-2479 , 2(2) (2012) PP. 68-90..
[26] Y.C. Hu A. Perrig and D. B. Johnson. *PACKET LEASHES*: A defense against wormhole attacks in wireless ad hoc networks. *IEEE INFOCOM*, pages 19
[27] Kiran B., Kareem S.A., Illamani V., Chitralekha S., "Case of Phthiriasis palpebrarum with blepheroconjunctivitis", Indian Journal of Medical Microbiology, ISSN : 0255-0857, 30(3) (2012) PP. 354-356..
[28] Dr.G.Brindha, A Study on Quality of Work Life of the Employees at Baxter (INDIA) Private Ltd., Alathur, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,612-615, Vol. 2, Issue 3, March 2013
[29] Dr.G.Brindha, An Analytical Study of the Proposed Voluntary Retirement Scheme in Bharat Sanchar Nigam Limited, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 2707-2712, Vol. 2, Issue 7, July 2013
[30] Dr.G.Brindha, BEYOND THE JUNGLE Strategic Information Systems Theory in 'Low –Competitive' Contexts, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 1446-1450, Vol. 2, Issue 6, June 2013
[31] Dr.G.Brindha, Mergers and Acquisitions, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp1446-1450, Vol. 2, Issue 11, November 2013
[32] Dr.G.Brindha, Building Competitive Advantage through Links with Science, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 1154-1164, Vol. 2, Issue 4, April 2013
[33] Dr.G.Brindha, Article on Portfolio Management, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 2182-218, Vol. 2, Issue 6, June 2013