International Journal of Advanced Trends in Computer Applications
www.ijatca.com

ANALYTICAL REVIEW OF AODV IN WORM HOLE ATTACK

Kanika Arora[1], Sonia Jindal[2]
[1] KanikaArora
Mtech Student
Chandigarh Engineering college , Landran (Mohali), Punjab
Kanilisa@gmail.com
[2] Sonia Jindal
Assistant Professor
Chandigarh Engineering College , Landran (Mohali), Punjab
cecm.ece.nsm@gmail.com

Abstract: *In era of wireless device, MANET are becoming more and more common due to current enhancements .There will be no centralized authority to manage the network .MANET is used for tracking and monitoring the attended environment, as nodes are small with limited resources as well as highly mobile .Communication among nodes is accomplished by different routing protocols .But these protocols have different security flaws and attack. Worm hole attack is one of the serious threat in context of Ad Hoc Network, thereforeis typically challenging to defend and frequently occurred in wireless systems. In this paper, impact of Worm Hole Attack and its operation on AODV protocol is analyzed.*

Keywords: *MANET, Routing Protocol, Attacks, Worm Hole Attack, AODV*

I. Introduction

Mobile Ad-hoc Network (MANET) is a recent enhancement which satisfies us from expensive deployment cost. It is self configurable without fixed network infrastructure and centralised administration. Previously Adhoc network research were on problems like protocol establishment and routing , assuming a faithful environment .However many applications run on an un faithful environment and require secure and trusted communication for example in rescue and emergency operation like flood ,tornado and earthquake or in military conditions . However, the wide nature of the wireless communication channels, the infrastructure less wireless network rapid deployment and the hostile environment where they may be deployed, make harm to a wide range of security attacks [15]. Many existing routing protocols in MANETs i.e. AODV(Ad hoc on demand distance vector) proposed by Perkins, Belding Royer & Das, 2003 and DSDV(Destination sequenced distance vector) proposed by Perkins & Bhagwat,1994 are prone to a variety of attacks that can degrade and harm the performance of the whole network and thus pose serious threat to security of such networks. A particularly severe security threat called the wormhole attack and its operation in AODV has been introduced in the context of ad hoc networks. Figure 1 shows a simple mobile ad hoc network. As MANETs are illustrated by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes.

Figure-1: A mobile Ad Hoc Network

II. Literature Survey

Yih-Chun Hu et al. proposed Packet leash technique .It is used to restrict the maximum transmission distance of packet,some information is added .Two kinds of packet leashes: geographic leash and temporal leash are defined . The geographic leash ensures that packet has upper bound on the distance, whereas the temporal leash computes that a packet has an upper bound on its lifetime.[16]

Unlike Packet Leash, Capkun et al. [8] proposed Sector(Secure tracking of node encounters in multi hop wireless networks) which does not need any synchronization of clocks and any kind of location informationfor the secure verification at time of encounters between nodes with the help of Mutual Authentication with Distance-Bounding technique These protocols are built on well defined cryptographic techniques, which includes hash chains and merkle hash trees.

Jane Zhen and Sampalli proposed Round Trip Time (RTT) mechanism. The RTT is the time that initiates from the Route Request (RREQ) packet transmitting time of a node A to Route Reply (RREP) packet receiving Time from a node B. A will calculate the RTT between A and its each and every neighbour.

Sun Choi et al. [7] proposed an efficient method which is Wormhole Attack Prevention (WAP) without using any hardware. In WAP all nodes having special list i.e its neighbour list computes and monitors the neighbour behaviour when they transmit RREQ (Route Request) messages to the destination. Therefore to prevent them from taking part in routing again, we store worm hole nodes information at the source node.

Uma Rathore et al. [6] presented an energy efficient routing protocol. EERP (Energy efficient routing protocol) is proposed which is based on AODV protocol. EERP protocol decreases the transmission power of a node if next hop node is closer which part of an active route is. The distance between two consecutive nodes during route reply is calculated by RSS (received signal strength) from next hop .

Trust and Reputation technique exploits worm hole nodes and its packet dropping property. TARF which is a trust aware routing framework demonstrates the trust level and efficiency of each neighbour node and worm hole nodes are considered if trust level of node is least [5].

III. Overview of Routing Protocol

The MANET's nature makes simulation modelling precious equipment for defining the operation in networks. In order to calculate a defined path between source and destination, Multiple Ad-hoc network routing protocols have been proposed in previous years. S. R Jathe& D. M Dakhane [14] described that in a network of two or more computers, a set of instructions or a common set of rules is required that each computer should follows to communicate with each other. Such a set of instructions or rules is called PROTOCOL. Depending upon, by which computers can communicate, the routing protocols can be divided into three categories [1] .

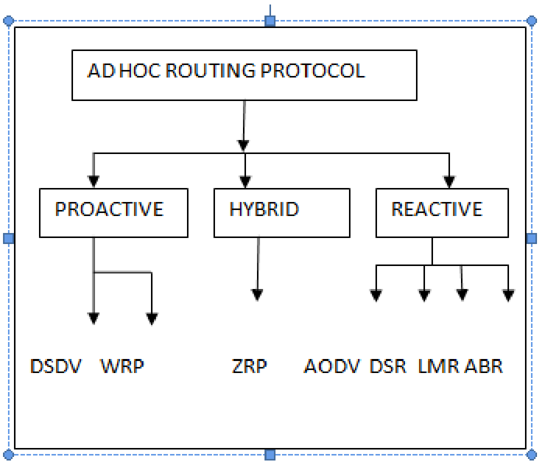


Figure -2: Classification of Routing Protocols

3.1 Proactive (Table Driven Protocol)

This Proactive protocol maintains the routing information even before it is needed. Routing information is maintained by each and every other node in the network. Routes activity and related information is stored in the routing table and is periodically updated as the network topology changes. Example of this protocol is DSDV (Destination Sequenced Distance Vector).

3.1.1 Destination-Sequenced Distance Vector (DSDV)

It is also called table driven protocol. It was proposed by C. Perkins and P. Bhagwat in 1994, to solve the routing loop problem. Routes are created for constant traffic control and are available every time even if there is no communication. Each and every node continuously maintains and update tables to provide new view of whole network. The disadvantage of DSDV is updation and maintenance of the tables. Improved functions of DSDV have been declared, but commercial forms has not yet been done.

3.2 Reactive (On Demand routing protocols)

These protocols maintain routing information and its activity at the network nodes only if there is communication. If there is transmission of packet from one node to another then identification of path is done and route is established in on demand manner. Examples of this protocol is AODV (Ad Hoc On-Demand Distance Vector).

3.2.1 Ad-hoc on–demand distance vector (AODV)

It is a reactive protocol that reacts on demand. It is a modification of DSDV. AODV has low memory overhead, builds unicast routes from source to the destination and network utilization is less. Since routes are built on demand, there is least routing traffic in the network. When two nodes in an ad hoc network wants to establish a connection between each other, it will build multihop routes. The main advantage of AODV is its least congested route instead of the shortest path. Route discovery and Route maintenance are two basic operations of AODV and it uses Route Request, Route reply and Route error messages for the same. In Route discovery phase, when source node does not not have a path to destination, it broadcast RREQ(Route Request) message which constitutes source and destination IP address , sequence number, hop count and its broadcast ID Neighbour node which receives RREQ transmits RREP (Route Reply), if it has either path to destination or is destination itself. Source node will transmit data through forward route. In route maintenance phase, when link failure is detected then it transmits RERR (Route Error) messages to source node. If source node has still data to send then it will reinitiate the route discovery process. RREQ and RREP packets are as described in Table 1 and Table 2.

Table 1: RREQ

Source Addre ss	Source Sequen ce	Broad cast ID	Dest Addres	Dest seque nce	Hop count

Table 2: RREP

Source Address	Destination address	Destination Sequence	Hop Count	Lifetime

Source Address: The address of the node which originated the route request.

Source Sequence: The current sequence number to be used for route entries pointing to the source of the route request.

Broadcast ID: A sequence number which uniquely identifies the particular RREQ when taken in conjuction with source node's IP address.

Destination address: The address of destination for which a route is desired.

Destination Sequence: The last sequence number in the past received by the source towards the destination for any route.

Hop Count: It is number of hops from source IP address to the node which handles the request.

Lifetime: The time for which nodes receive the RREP messages are considered the route to be valid.

3.3 Hybrid routing protocols

Hybrid routing protocols combine proactive routing protocols with reactive routing protocols. In order to establish the best paths to destination networks, they use distance-vector for more precise metrics and report routing information only when there is a change in the topology of the network. Zone Routing Protocol (ZRP) is an example of a Hybrid routing protocol [3].

3.3.1 Zone Routing Protocol (ZRP) [2]

It aims to address the problems by combining the best properties of both approaches i.e proactive and reactive protocols .It can be classed as a hybrid proactive routing protocol. The Zone Routing Protocol, suggeststhat it deals with zoning concept. A routing zone explains each node individually , and the zones of neighbouring nodes overlap. Further the behavior of ZRP is adaptive. It depends on the current configuration of the network and the behavior of the users. [4]

Among all these protocols, AODV is being Considered as Secure protocol and used for energy efficiency. AODV is considered to be better for this criteria because it is on-demand with route maintenance phase in its process.

IV. Categorizing Attacks In Manet

A) Active Attacks

In this the attackers replicate , modify , alter, and delete the exchanged data. These attack change protocol's behaviour and try to harm flow of messages among the nodes.The intruder performs an effective violation on either the network resources or the data transmitted.These attack donot affect network's operation.

B) Passive Attacks

In this attackers does not effects the operation of routing protocol rather it is only audible to identify the secured information [9]. Passive attacks are categorized according to the functionalities in layers in the protocol stack.

- **Transport Layer Attack**

Session Hijacking: Attackers in session hijacking harms the session which is not protected after its first setup. In this attack, verification of victim's node IP address, identification of correct sequence number is verified. In Session hijacking, the false node gets its protected data which is passwords, log in names and other critical information from nodes.

- **Application Layer Attack**

Repudiation attacks: It refers to a denial of participation in all parts of the communication .By denying the communication some nodes may behave as selfish nodes .Example of this attack is spyware detection software which is used in mission critical services.

- **Multilayer Attack**

These are not associated with single layer in the protocol stack.

Denial of service attack*:* Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network [10].

- **Blackmail**

This attack is a consequence of lack of authentication and it permits provision to nodes so that they can corrupt and duplicate some other node's useful information. This attack is useful in area that identifies malicious nodes and in propagation of messages that try to blacklist the offender

- **Black Hole Attack**

Malicious nodes monitor the routing request in the network and advertise themselves as the centered nodes that have shortest paths to the destination nodes. A false route is created, when reply from malicious nodes reaches the source. Then if the communication is started then malicious nodes get the data from the transmitter node and data can be dropped or altered.

- **Wormhole Attack**

Wormhole attack is a tremendous threat in Wireless networks. Where various attackers are linked by high speed off-channel link termed as wormhole link [12]-[13].Both attackers creates 'tunnels' to forward the data packets and broadcast packets into the network. The worm hole attack has a serious consequences in the network.

In the figure nodes K and L are colluding nodes that create wormhole tunnel. When finding the route from the node S to D, node K receives RREQ packet and creates an illusion that node L is a neighbour node of node K that has shortest path to the node D.

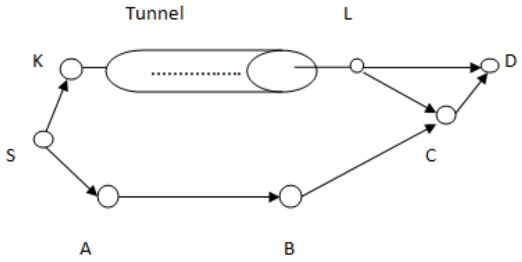
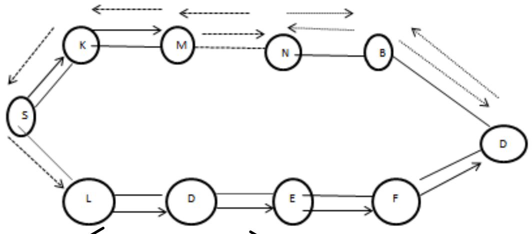


Figure 3: Example of Worm Hole Attack

V. OPERATION OF WORM HOLE ATTACK IN AODV

Wormhole attack is a type of replay attack and is seriously challenging in MANET to defeat against. It can be very effective and damaging, even if the data included in routing is private, confidential or authenticated. It affects the original functionality of routing protocols like AODV, DSR and OLSR etc, but this paper emphasizes on wormhole attack in AODV routing protocol.



→ RREQ ← RREP ⇢ RREQ through wormhole

— Wireless link ------ Wormhole link

Figure 4: Wormhole attack in AODV

Wormhole attack [11] in AODV consists of two remote false nodes which is malicious nodes labelled as M and N in Figure 4. M and N both are linked by wormhole link and both of them targeted S which is source node .To do so , it tunnels the received message with the help of low latency links to its opposite end . During path discovery phase, S will broadcast route request (RREQ) message to end i.e destination node D. So K and L are in neighbourhood of S, which will receive and then transmit Route request message to its neighbours. Now the false node M is forwarded by K that receives RREQ. It records and tunnels the RREQ for its partner N. False node N then transmits Route Request message to B. At the end, B transmits it to destination D. Thus, path is follows as S-K-M-N-B-D and RREQ is broadcasted in this route. Other path can be S-L-D-E-F-G-D and RREQ is broadcasted .But M and N are connected through worm hole link and it attracts traffic towards them , so route request from path S-K-M-N-B-D has reached first towards D. Therefore, destination D are mislead and leaves the path that arrive later and chooses first path D-B-K-S to unicast message to the source node S. As a result, first path has false node M and N which are malicious and mislead other nodes in the network. Thus, a wormhole attack can be immensely harmful for a MANET, but still it is not that difficult to set up. However, finding better techniques and securing AODV for detection of wormhole attacks still remains a bigthreat.

VI. CONCLUSION

MANET needs a trustworthy, efficient, scalable and secure protocol as they are highly insecure. To be supported by nodes in MANETs, the memory and computational cost is reasonable enough. At various level, researchers prevent ad hoc network from certain attacks and threat. Various types of such attacks have been explained in this paper. We conclude Worm Hole Attack is very serious threat and it must be treated as highest priority attack.

References

[1]Kannhavong, Bounpadith, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour. "A survey of routing attacks in mobile ad hoc networks." *Wireless communications, IEEE* 14, no. 5 (2007): 85-91.

[2]Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: Intrazone Routing Protocol (IARP), June 2001, IETF Internet Draft, draft-ietf-manet-iarp-01.txt

[3]Shiva Prakash, J. P. Saini, S. C. Gupta," A review of Energy EfficientRouting Protocols for Mobile Ad Hoc Wireless Networks"InternationalJournal of Computer Information Systems, Volume 1, 2010.

[4]Pearlman, Marc R., Haas, Zygmunt J.: Determining the Optimal Configurationfor the Zone RoutingProtocol, August 1999,IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8

[5]Guoxing Zhan, Weisong Shi, Julia Deng, "Design and Implementation of TARF:A Trust-Aware Routing Framework for WSNs", *IEEE Transactions on dependable and secure computing*, pp 1545-5971(2012)

[6] Bhatt, Uma Rathore, Priyanka Jain, and RakshaUpadhyay. "Enhanced AODV—An energy efficient routing protocol for MANET." In *Engineering (NUiCONE), 2013 NirmaUniversity International Conference on*, pp. 1-4. IEEE, 2013.

[7] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, pp. 343-348

[8] S. Capkun, L. Butty´an, and J.-P.Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pages 21–32, Oct 2003.

[9] MahaAbdelhaq, Rosilah Hassan, Mahamod Ismail, RaedAlsaqour, DaudIsraf, *Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm,* International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).

[10] PriyankaGoyal,SahilBatra , Ajit Singh, *A Literature Review of SecurityAttack in Mobile Ad-hoc Networks*, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[11] Rashid HafeezKhokhar, MdAsriNgadi and Satira Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3

[12] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 14 Proceedings of the 11th Network and Distributed System Security Symposium, 2003.

[13] Y.-C. Hu, A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

[14]S. R. Jathe, and D. M. Dakhane, "Indicators for Detecting Sinkhole Attack in MANET", *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, pp. 2250-2459, Jan. 2012

[15]Jawandhiya, Pradip M., et al. "A survey of mobile ad hoc network attacks." *International Journal of Engineering Science and Technology* 2.9 (2010): 4063-4071.

[16]Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. IEEE INFOCOM, Mar 2003.