Comparative Study of Attacks with Clustering based and Routing Protocols in MANETs

Harmanpreet Kaur
PG Student
Chandigarh Engineering College
Landran , Punjab , India

Sunidhi Sharma
Asstt. Prof., Department of CSE
Chandigarh Engineering College ,
Landran , Punjab , India

ABSTRACT
A mobile ad-hoc network is a self-configuring, substructure network of mobile devices associated by wireless links. Loopholes like wireless average, lack of a secure infrastructure, dynamic topology, rapid disposition practices, and the hostile surroundings in which they may be deployed, make MANET susceptible to a wide range of security attacks and Wormhole attack is one of them. During this attack malicious node detentions packets from one location in the network, and channels them to another colluding malicious node at a detached point, which replays them locally. The protocol is an optimization of the traditional link state algorithm personalised to the supplies of a mobile wireless LAN. The key concept used in the procedure is that of multipoint relays. MPRs are selected nodes which advancing broadcast messages during the flooding process. This technique significantly reduces the message overhead as associated to a classical flooding apparatus, where every node retransmits each message when it receives the first copy of the message. In OLSR, link state information is caused only by nodes elected as MPRs. Thus, a second optimization is achieved by reducing the number of control messages flooded in the network. This paper presents a cluster based Wormhole attack prevention technique. The concept of classified clustering with a novel hierarchical 32- bit node addressing scheme is used for eluding the attacking path during the route discovery phase of the OLSR protocol, which is measured as the under lying routing protocol.

Keywords
Worm Hole Attack, optimized link source routing, Wireless Sensor Network, Local Area Network,Re-active and Pro-active protocols.

1. INTRODUCTION
Wireless Mobile Ad-hoc Network is a self-configuring network which is collected of some movable user apparatus. These mobile nodes communicate with each other without any organization, additionally ;all of the transmission links are recognised through wireless medium. According to the communiqué mode declared before[1]. MANET is extensively used in martial purpose ,disaster area, particular area network and so on. However, there are motionless many open problems about MANETs, such as refuge problematic, finite transmission bandwidth, abusive spreading messages, dependable data delivery, dynamic link formation and constrained hardware caused processing abilities.

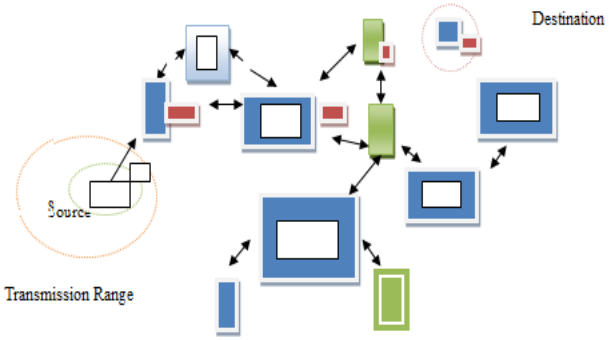

Fig 1. Mobile Ad-hoc Network [1]

A MANET contains of numerous mobile nodes that are linked by wireless associations and each mobile node acts not only as a host but also as a router to found a route. When a source node proposes to transmission the data packets to the destination node, then the packages are relocated through transitional nodes, thus speedy deployment of the nodes to found a route is the important matter in MANET.

2. RELATED WORK
Zubair Ahmed Khan et al., 2012[2]displayed that the routes in the routing table have not been used for the discovery of the wormhole attack; with a little alteration to the structure of the routing table we can be able to detect apprehensive links. In this paper they had proposed the use of the modified routing table for detection of the suspicious links, authorisation of wormhole presence, at the end isolating the established wormhole nodes. **Subhashis Banerjee et al., 2014[3]**presented a hierarchical cluster based Wormhole attack prevention technique to avoid such scenario. The perception of hierarchical grouping with a novel hierarchical 32-bit node addressing scheme is used for escaping the attacking path during the route discovery segment of the DSR protocol, which is measured as the under lying routing protocol. Pinpointing the location of the Wormhole nodes in the case of uncovered attack is also given by using this method. **PoonamDabas et al., 2013[4]** described as, security

has become a major concern in order to provide endangered communication between mobile nodes in an aggressive environment. The lack of any central coordination apparatus and shared wireless medium makes MANETs more susceptible to cyber-attacks than wired network. Different appliances have been proposed using various cryptographic methods to countermeasures these attacks in contradiction of MANET. The Wormhole attack at network layer is the most attention looking for attack in ad hoc networks. This attack is tough to detect and easy to appliance. **Mariano García-Otero et al., 2012**proposed [5] two wormhole exposure procedures for WSNs, based on impressions employed in kind of range-free localization methods: one of the methods performs the detection instantaneously with the localization procedure, and the other activates after the deduction of the location discovery protocol. Both strategies are effective in detecting wormhole attacks, but their presentation is fairly sensitive to investigation effects present in the radio channels.

3. WORM HOLE ATTACK

Wormhole is a proposed shortcut through universe and time that connects two detached regions. The Wormhole attack at network layer is the most consideration seeking attack in ad hoc networks. Wormhole attack is also recognized as tunnelling attack. In a wormhole attack, the attacker accepts packets at one location in the network, shafts them [6] to another position and replays them there. This tunnel between two plotting attackers is referred to as a Wormhole. It could be recognized through wired link between two colluding attackers or through a single long-range wireless link. This attack is hard to detect and easy to instrument. In this form of attack the attacker may generate a wormhole even for packets not talked to itself because of broadcast nature of the radio station.

In the fig. under, the path from Source to Destination via wormhole link has the length of 5 when the standard path has the length of 11. Therefore, in most routing protocols, Source wishes sending data to D along the path with wormhole link [7]. The Wormhole attack can be classified into two categories:

1) Hidden attacks and

2) Exposed attacks,

Depending on whether wormhole nodes put their individuality into packet's headers when tunnelling replaying packets.

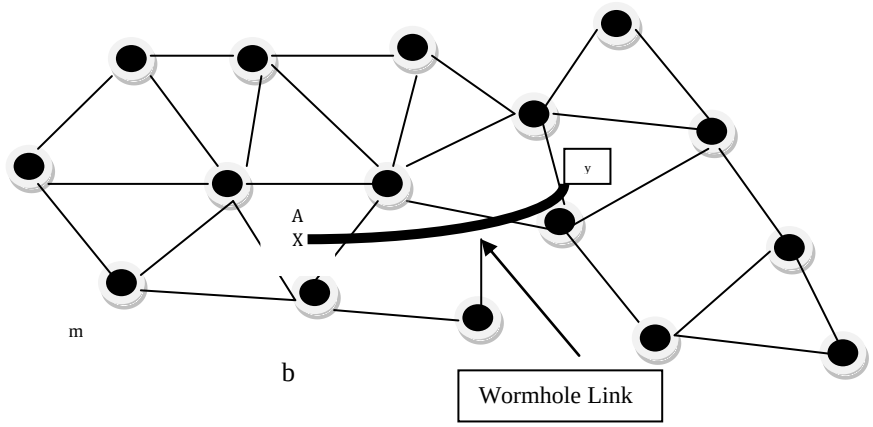

Fig 3. Worm Hole Attack

3.1 Cluster Based Approach For Worm Hole Attack

Clustering algorithm is to confirm the occurrence of wormhole attack and find the mischievous nodes. Using hop count and timing enquiry, the presence of wormhole link along the route can be supposed. Once a route is supposed to have a wormhole link, the nodes along the route act as CH, which first groups all its one-hop neighbours. For cluster formation and localization of wormhole attack, the remaining routing table should be modified to add an extra field, which is used to check whether a neighbouring node is a cluster member or not [10]. All nodes which are in one-hop vicinity of the CH will be in the cluster of that node, except the next node along the route. For adding the next node along the route, some more authorization tests are to be done, to assure that the node is genuine. After cluster formation, two special control packets CREQ and CREP are used for confirming and restricting the presence of wormhole attack along the route.

An algorithm where intrusion discovery has been done in a cluster based method to take care of the wormhole attacks. The AODV routing protocol is usedas the fundamental network topology. A two layer approach is used for detecting whether a node is contributing in a wormhole attack. The layered approach is introduced to reduce the load of processing on each cluster heads. From security point of view, this will also decrease the risk of a cluster head being compromised.

The clusters may be overlay or disjoint. Each cluster has its own cluster head and a number of nodes chosen as member nodes. Member nodes pass on the information only to the cluster head. The cluster-head is accountable for passing on the aggregate information to all its members. The cluster head is elected vigorously and maintains the routing information.

Assumptions:

- Key generation, distribution and management are secure.
- It is not possible for a node to copy the digital signature of a Cluster Head.

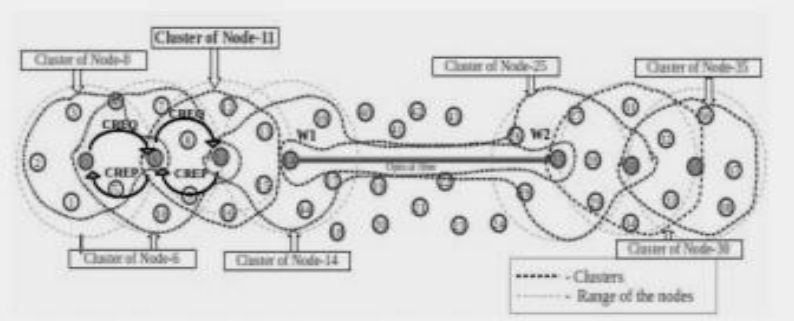

Fig 3. Cluster Head

4. ROUTING PROTOCOLS

Two types of routing protocols:

a) Proactive and

b) Reactive Routing Protocol

i) Table driven Routing Protocol

The pro-active direction-finding is also called [8] table-driven routing protocol. In this routing protocol, mobile nodes occasionally transmission their routing information to the neighbours . Each node needs to preserve their routing table which not only archives the adjacent nodes and accessible nodes but also the number of hops. In other words [9], all of the nodes have to calculate their neighbourhoods as long as the network topology has developed. Therefore, the trouble is that the overhead rises as the network size surges, an important communication overhead within a superior network topology.

ii) Reactive Routing Protocol

The reactive routing is equipped with another appellation named on-demand routing protocol. Different the pro-active routing, the responsive routing is simply started when nodes desire to transmit data packets [9]. The strength is that the misused bandwidth encouraged from the cyclically broadcast can be reduced. Nevertheless, this might also be the deadly wound when there are any spiteful nodes in the network environment.

Table no: 1 Comparison between Routing Protocols

Protocol	Update destination	Update time	Advantages/disadvantages
AODV	Source	Event driven	1.Reduced overhead 2.Periodic Updates
DSR	Source	Event driven	1.R educed load 2.high delay
ABR	Source	Periodically	1. Avoid packet duplicates. 2.process complexity
OLSR	Source	Table Driven	1.Flat Routing Protocol 2.Increase topology bandwidth

4.1 An Overview Of OLSR (Optimized Link Source Routing)

The technique of OLSR is as follows. Every node transmissions HELLO messages that contain one-hop neighbour information periodically. The TTL of HELLO [11] messages is 1, so they should not forwarded by its nationals. With the aid of HELLO messages, every node finds local topology information. A node chooses a subdivision of its neighbours to act as multi-point relaying nodes for it is based on the local topology info, which are specified in the intermittent HELLO messages later. MPR nodes achieve two tasks: (D when the selector sends or forwards a broadcast packet, only its MPR nodes among all its neighbours advancing the packet the MPR nodes periodically broadcast its chooser list throughout the MANET (again, by resources of MPR flooding). Thus every node in the Network knows through which MPR nodes every other node could be touched. With global topology information stored and efficient at every node, a shortest path from one node to every other node could be calculated with Dijkstra's algorithm, which goes along a series of MPR node.

4.2 Difference between of OLSR and AODV protocol

OLSR is also a flat routing protocol, it does not need central administrative system to handle its routing process. The proactive distinguishing of the protocol provides that the protocol has all the routing information to all contributed hosts in the network. However, as a drawback OLSR protocol needs that each host periodic sends the efficient topology information throughout the entire network, this increase the protocols bandwidth usage. But the flooding is diminished by the MPRs, which are only allowed to forward the topological messages.

The reactiveness to the topological changes can be adjusted by shifting the time interval for broadcasting the Hello messages. It increases the protocols suitability for ad hoc network with the quick changes of the source and destinations pairs. Also the OLSR protocol does not necessitate that the link is reliable for the control messages, since the messages are sent periodically and the delivery does not have to be sequential.

One disadvantage is that intermediate nodes can lead to inconsistent routes if the source arrangement number is very old and the middle nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple Route Request packets in response to a single Route Request packet can lead to heavy control overhead.

Fig a. OLSR Protocol

4.3 Ad-hoc Routing Protocol

The information in this segment concerning the Ad Hoc on Demand Distance Vector Protocol (AODV) protocol is taken from the RFC. AODV is a reactive protocol, i.e., so the ways are created and preserved only when they are desirable. The routing table supplies the information about the next hop to the destination and a sequence number which is received from the destination and representing the freshness of the received information. Also the information about the active neighbours is received through the discovery of the destination host. When the conforming route breaks, then the neighbours can be notified .The route discovery is used by distribution the RREQ message to the neighbours with the demanded destination sequence number, which prevents the old material to be replied to the demand and also prevents looping problem, which is essential to the old distance vector protocols. The route demand does not add any new information about the past hosts only it surges its hop metric. Each passed host makes update in their own routing table about the entreated host. This information helps the sink reply to be easily routed back to the requested host. The route reply use RREP message that can be only generated by the terminus host or the hosts who have the information that the destination host is alive and the joining is fresh.

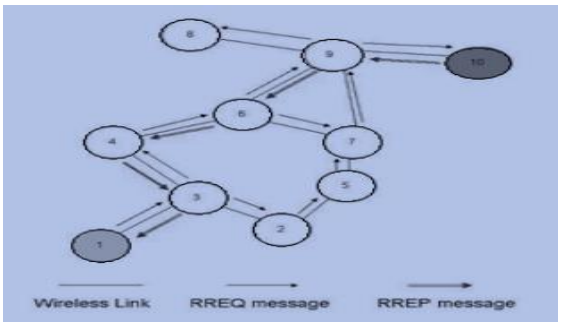

Fig. b AODV Protocol

5. CONCLUSION

Wormhole attack is a great risk in MANET, as it can disturb the entire communication. It is important to eliminate such exposures from the network and many surveys have been done to detect wormhole attack in MANET. Wireless medium's openness, every sensor can hear the shortest sensor or you can say neighbour radio without being detected. When many malicious sensors construct one or more wormholes, they can terminate network by disturbing the routing protocol, especially OLSR protocol. Wormhole attack detection is done in two phases.

a) First Phase of detection, hop count is used to clarify the presence of attack.
b) Attack is supposed along a path, a clustering approach is done to clear the presence of attack and the local attackers.
c) Clustering technique is effective to verify the presence of wormhole attack with optimizing error.

Both protocols scalability is limited due to their proactive or reactive distinctive. In the AODV protocol, it is the flooding overhead in the high flexibility networks. In the OLSR protocol is the size of the routing table and topological updates mails. After distrusting the attack, a Clustering based approach is used to confirm the attendance of attack, and also to identify the attacker nodes. The entire network is alienated into different clusters and each cluster will have a Cluster Head, which controls all the nodes in the cluster and plays the role of a controlling authority in MANET.

6. REFERENCES

[1] Al Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." Proceedings of the 42nd annual southeast regional conference. ACM, 2004.

[2] Khan, Zahoor Ali, and M. Hasan Islam. "Wormhole attack: A new detection technique." *Emerging Technologies (ICET), 2012 International Conference on*. IEEE, 2012.

[3] Banerjee, Subhashis, and KoushikMajumder. "ANovel CLUSTER BASED WORMHOLE AVOIDANCE ALGORITHM FOR MOBILE AD-HOC NETWORKS." *ICCSEA, SPPR, CSIA, WimoA–2013*.

[4] Dabas, Poonam, and PrateekThakral. "A Novel Technique for the Prevention of Wormhole Attack." *International Journal* 3.

[5] García-Otero, Mariano, and Adrián Población-Hernández. "Detection of wormhole attacks in wireless sensor networks using range-free localization."*Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2012 IEEE 17th International Workshop on*. IEEE, 2012.

[6] Clausen, Thomas, et al. "Optimized link state routing protocol (OLSR)." (2003).

[7] Banerjee, Subhashis, and KoushikMajumder. "WORMHOLE ATTACK MITIGATION IN MANET: A CLUSTER BASED AVOIDANCE TECHNIQUE."*International Journal of Computer Networks & Communications* 6.1 (2014): 45.

[8] Hao Yang, HaiyunLuo, Fan Ye, Songwu Lu, and Lixia Zhang, Security in Mobile Ad Hoc Network: Challenges and Solutions, IEEE wireless Commutations, February 2004.

[9] Umang S, Reddy BVR, Hoda MN (2010) Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption. IET Communications 4(17):2084–2094. doi: 10.1049/ietcom.2009.0616.

[10] Mbarushimana, Consolee, and Alireza Shahrabi. "Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks." Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. Vol. 2. IEEE, 2007.

[11] Anju, J., and C. N. Sminesh. "An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET." *Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference on*. IEEE, 2014.