Optimized Link State Routing protocol for Mobile Ad hoc Networks

[1]Deepshikha Yadav, [2]Vivek Gupta
[1,2]Department of Computer Science & Engineering
[1,2]Acropolis Technical Campus, Indore

***Abstract*— Mobile ad hoc network is collection of self configuring, autonomous nodes connected with wireless links. The mobile ad hoc network is an open network that is not depends on any fixed infrastructure or base stations. Mobile ad hoc networks are being widely deployed currently since they provide some features, which are difficult or impossible to be achieved by conventional networks. Hence mobile ad hoc networks are applicable to large areas from battlefield to general transportation which is very useful in disaster recovery. Due to the great importance of MANET, security in ad hoc networks is a hot research area and already significant research is done in this field. In this paper discusses a new routing algorithm for Mobile Ad hoc Networks to avoid "Worm-Hole" attack. Wormhole attack is most common attack in mobile ad hoc network and it degrades the performance of the routing protocol and then whole network. Optimized Link State Routing protocol is a proactive table driven routing protocol in mobile ad hoc network and it is also victimize by wormhole attack. Our enhanced optimized link state routing protocol can be used to detect wormhole attack in mobile ad hoc network that have some malicious nodes. The proposed protocol detects the nodes that forward packets to attackers based on frequency of use of each node. The basic purpose of the research is to give an efficient and secure proactive routing protocol for mobile ad hoc network.**

Keywords: Mobile Adhoc Network, Worm-Hole Attack, Routing protocols.

I. INTRODUCTION

A. Mobile Ad hoc Network Mobile ad hoc network is collection of self configuring, autonomous nodes connected with wireless links. The mobile ad hoc network is an open network that is not depends on any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. As shown in Figure.1.1, there are no base stations and every node must co-operate in forwarding packets in the network.

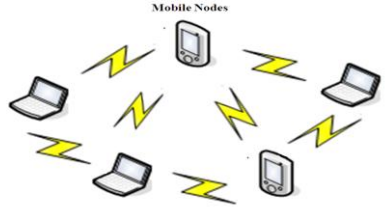

Figure 1.1 A Mobile ad hoc Network

Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes. The wireless environment of mobile ad hoc network is the reason for lots of security threats. The most common security threats are denial of service attack, rushing attack, black hole attack, wormhole attack, gray-hole attack etc. These threats become sever when they target the network routing protocols. Proactive/table-driven and reactive/on-demand both type of routing protocol is vulnerable to these security attacks. The attacks on these routing protocols are routing table overflow, routing table poisoning, packet replication, route cache poisoning, rushing attack etc. These attacks can either be performed by internal or external nodes. An external attacker is any unknown node comes in vicinity of mobile ad hoc network and performs malicious activities and an internal attacker is a legitimate node compromised by attacker. The attack performed by internal attacker is difficult to detect because sometime they acts as malicious node and sometime behave as legitimate node. There are many research has been done to deal these security threats

B. Advantages of Mobile Ad hoc Networks

Having discussed the general issues in MANETs, the reason behind their popularity and their benefits will now be discussed.

- *Low cost of deployment*: As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.
- *Fast deployment*: When compared to WLANs, ad hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.
- *Dynamic Configuration:* Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in classrooms, etc., this is a useful feature.

C. Applications of Mobile Ad hoc Networks

Adhoc networks have several interesting applications ranging from battlefield to class rooms. In this section, some scenarios of deployment are discussed.

(a) Battlefield: In a battlefield, communication between soldiers and vehicles can be carried out using ad hoc networks. In such networks, the soldier troops might communicate with each other using hand-held devices. The vehicle mounted

devices can be equipped with power sources for "recharging" these mobile devices.

(a) Rescue Operation: In scenarios such as fire fighting or avalanche rescue operations, a quick deployment of nodes is required. Ad hoc networks can be used in such scenarios for communication between the workers.

(b) Event Coverage: Scenarios such as a press conference might entail reporters to share data amongst other reporters. In such cases, multimedia traffic might be exchanged between nodes such as laptops, PDAs, etc.

(c) Classroom: In a classroom, students and instructors can set up an ad hoc wireless network to share data using laptops.

D. **General Issues in Mobile Ad hoc Networks**

In a mobile ad hoc network, all the nodes co-operate amongst each other to forward the packets in the network and hence, each node is effectively a router. Thus one of the most important issues is routing. In this section, some of the other issues in ad hoc networks are described.

(a) *Distributed network:* A MANET can be considered as a distributed wireless network without any fixed infrastructure. By distributed, it is meant that there is no centralized server to maintain the state of the clients, similar to peer-to-peer (P2P) networks.

(b) *Dynamic topology:* The nodes are mobile and hence the network is self-organizing. Due to this, the topology of the network keeps changing with time. Hence the routing protocols designed for such networks must also be adaptive to the changes in the topology.

(c) *Power awareness:* Since the nodes in an ad hoc network typically run on batteries and deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life, or in other words, they must be power aware.

(d) *Addressing scheme:* The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology entails a ubiquitous addressing scheme, which avoids any duplicate addresses. Mobile IP is currently being used in cellular networks where a base station handles all the node addressing. However, such a scheme doesn't apply to ad hoc networks due to their decentralized nature.

(e) *Network size:* Commercial applications of ad hoc networks such as data sharing in conference halls, meetings, etc. are an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.

(f) *Security:* Security in an ad hoc network is of prime importance in scenarios of deployment such as battlefield. The three goals of security - confidentiality, integrity and authenticity are very difficult to achieve since every node in the network participates equally in the network.

E. **Routing Protocols in Mobile Ad hoc Networks**

Routing is the main step of a communication network. In wired network all the nodes are connected to a router and only router decides which route will be further followed by packet. As well as topology of wired network change rarely. So routing protocols can maintain the route in table at once and it remains valid for long time until network topology remains same.

Whereas in wireless network especially in ad hoc networks have dynamic topology and each node acts as a router. Hence routing protocol must be adoptive to dynamic topology and secure from threats. Routing protocols in Mobile ad hoc networks can generally be divided into three groups.

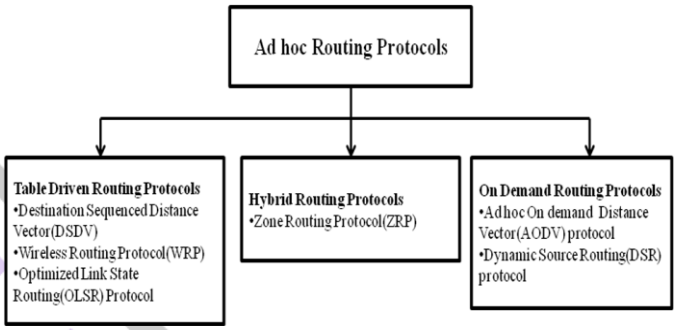

Figure 1.2 MANET Routing Protocol Classification

- **Table driven (Proactive) Routing Protocol:** Every node in the network maintains complete routing information about the network by periodically updating the routing table. Thus, when a node needs to send data packets, there is no delay for discovering the route throughout the network. This kind of routing protocols roughly works the same way as that of routing protocols for wired networks.

- **On demand (Reactive) Routing Protocol:** In this type of routing, a node simply maintains routes to active destination that it needs to send data. The routes to active destinations will expire after some time of inactivity, during which the network is not being used. The protocol comes in this category require initial delay to find route whenever needed.

- **Hybrid Routing Protocol:** This type of routing protocols combines features of the above two categories. Nodes belonging to a particular geographical region or within a certain distance from a concerned node are said to be in the routing zone and use table driven routing protocol. Communication between nodes in different zones will rely on the on-demand or source-initiated protocols.

II. OBJECTIVE

Ad-hoc or spontaneous wireless networks are threatened by a powerful attack known as the wormhole attack. Wireless networking is a young technology and thus, many wireless network devices have not been designed to defend against wormhole attacks. A wormhole attack can be set up with relative ease, but preventing one is difficult. To set up a wormhole attack, two or more attackers who are multi hop away create a tunnel and pretend themselves as neighbor to each other as shown in Figure 2.1.

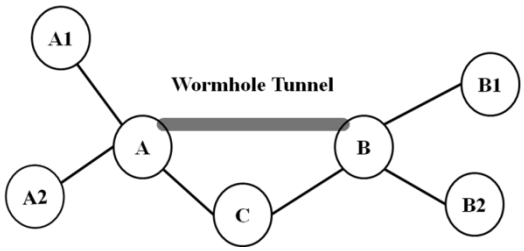

Fig. 2.1

After setting up a wormhole, an attacker can disrupt routing to direct packets through the wormhole tunnel for the purpose of drop modify or duplicate.

A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network. Almost each network protocol is vulnerable to wormhole attacks. A few solutions to detect wormhole attacks are presented but they require highly specialized equipment not found on most wireless devices. These solutions require time synchronization and location information of each node.

Our work is based on Optimized Link State Routing protocol in mobile ad hoc network. This work proposes an enhanced optimized link state routing protocol which provides security against wormhole attack in mobile ad hoc networks (MANET).Optimized link state routing protocol is specially developed for large and dense wireless ad hoc network where communicating peers changes over time. OLSR protocol is also vulnerable to wormhole attack. In the wormhole attack, a hostile node monitors the channel consciously, records packets overheard in its floor, and tunnels them to a remotely located colluding node, who will replay them in its floor. When this tunneling concerns specifically OLSR control packets, such as HELLO messages and topology control (TC) messages, nodes that are close to the attackers would be unable to discover the legitimate routes between the floor of the source attacker and the floor of the remote attacker, because such legitimate routes would span a larger number of hops than the one or two hops declared by the wormhole. This will severely disrupt communications.

The main aim of attackers is to pass all traffic through this wormhole tunnel so that attacker can drop, modify or duplicate the packets. Our proposed wormhole attack detection solution uses this characteristic of wormhole attackers. In this solution each node maintains frequency of use parameter called frequent appearance count of their neighbors. Each node monitors their neighbors that how many number of times their neighbor participate in routing to forward data packets from source to destination. If at all frequent appearance count of a node is more than threshold value that node is assume to be in route to wormhole tunnel. This information is spread in whole network so that no any other node will further use that node to forward data packets.

The proposed protocol neither requires clock synchronization of nodes nor any location information of nodes. It is a simple and efficient proactive routing protocol free from wormhole attack.

III. PROPOSED METHODOLOGY

In this section will explain overall methodology to be adapted for entire development. It contains overall functioning of Optimized Link State Routing protocol, wormhole attack in OLSR protocol, statistical analysis of effect of wormhole attack and proposed optimized link state routing protocol.

A. Optimized Link State Routing (OLSR) protocol for Mobile Ad hoc Networks

Optimized Link State Routing (OLSR) protocol is a proactive/table driven routing protocol developed specially for mobile ad hoc network. It is based on classical link state protocol used in wired network. Each node has topological information of whole network. Hence the route is immediately available when nodes want to communicate. OLSR protocol uses hop count as a matrix to find shortest path between source and destination. The nodes exchange topology information to each other periodically using two control messages i.e. HELLO and TC (Topology Control). These control messages is used to discover and disseminate topological information in the network. OLSR compact the size of information sent in the messages and furthermore reduces the number of retransmissions to flood these messages in entire network. Multi Point Relay (MPR) is used to flood control messages efficiently and economically. MPR nodes are subset of neighbors of any node, only which retransmit broadcast messages received from that node.

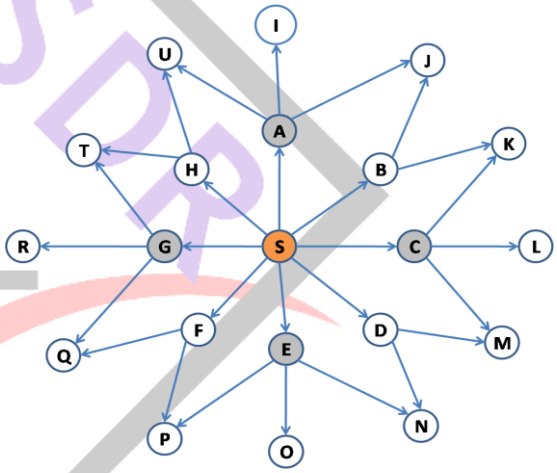

Fig. 3.1 OLSR Flooding

In Fig 3.1, we have a scenario in which a node S chooses a subset{A,C,E,G} of nodes from its neighbor set{A,B,C,D,E,F,G,H} as its Multipoint Relay(MPR) set such that all two hop neighbor I,J,K,L,M,N,O,P,Q,R,T,U will be covered to forward all control messages. In this way a limited flooding is performed in OLSR protocol. MPR nodes are nodes that have willing to forward control packets. Each node maintains following repository to perform routing:

- Link Set-keeps information about links.
- Neighbour Set-keeps information about neighbours.
- 2-hop Neighbour Set-keeps information about 2-hop neighbours.
- MPR Set-keeps information about nodes selected as MPR.
- MPR Selector Set-keeps information about nodes who selected any node as its MPR.
- Topological Information Base-keeps whole topological information.

- Routing Table-keeps information about shortest route to any destination.

i. Protocol functioning:

Step 1.Link Sensing: All nodes periodically broadcast HELLO packet to perform link sensing and maintain Local Link Set. As a result all links and their type (symmetric, asymmetric) between a node and its neighbor is discovered. The flow of HELLO messages for link sensing is shown in Fig3.2.

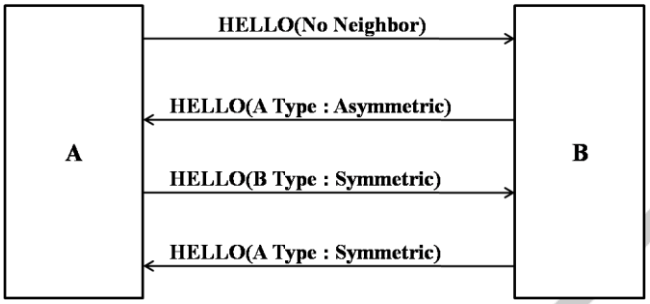

Fig 3.2

Step 2.Neighbor Detection: The information contain in HELLO message is also used to maintain Neighbor set, 2-hop neighbor set, MPR set and MPR selector set. Neighbor set contain address of neighbor node, status of its connecting link and its willingness to transfer packets. 2-hop neighbor set contain address of 2-hop neighbor, address of neighbor through which 2-hop neighbor has symmetric link.

MPR computation is performed to find out a subset from neighbor nodes which has willing to forward routing packets. These MPR nodes choose as they cover all 2-hop neighbor of any node. The MPR selector set is maintained on each node using neighbor type information contained in received HELLO message. If neighbor type is MPR_NEIGH then add sender as multipoint selector node.

Step 3. Topology Discovery: Topology Control (TC) message is used for topological discovery. Each node which has been selected as MPR advertize its MPR selectors using TC message. The information diffused in the network by these TC messages will help each node calculate its routing table.

Step 4.Routing table computation: Each node maintains a routing table which allows it to route data, destined for other nodes in the network. It is based on local link information base and topology set. Routing table contain address of destination node, address of one hop away node from local node, number of hops destination node away from local node and address of local node. Once routing table has been established, it must be modified when there is any change in network topology.

ii. Wormhole attack in OLSR:

Wormhole attack is one of the most sophisticated forms of the routing attacks in MANET. In this attack, an attacker records packets at one location in the network and then tunnels them to another location, where it is retransmitted by a colluding attacker. As a result, two far away nodes consider themselves as direct neighbors and then may select each other as MPR node. The tunnel can be established by using an out-of-band link, a wired link, or a logical link via packet encapsulation. In wormhole attack, an attacker can silently tunnel packets which are not even addressed to it. Since a wormhole attack can heavily affect the topology construction, it may be lethal to many ad hoc routing protocols, especially for proactive routing protocols such as OLSR, which periodically allows exchange of control packets for neighbors discovery and topology construction.

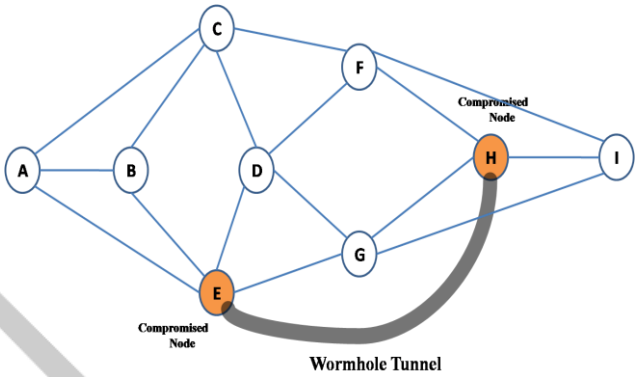

Fig3.3

A wormhole attack scenario is presented in fig 3.3, where E and H are compromised nodes which create wormhole tunnel using packet encapsulation. One of compromised node E receives all HELLO packets from node B, D and A, passes it through tunnel and further rebroadcasted by node H to node F and I. Similarly the HELLO messages received by compromised node H is tunneled to node E and further rebroadcasted to node B,D and A.As a result node B and I, D and I,A and I, B and F,A and F assume themselves neighbors of each other. And node A, B and D will choose node F and I as its MPR and vice versa. Hence some TC packets and data packets will pass through wormhole tunnel E-H. Due to this wrong neighbor detection and topology discovery, wrong topology information spread in the network, this leads to routing disruption and ultimately results in performance degradation of the ad hoc network as a whole.

B. Proposed enhance Optimized Link state routing protocol:

In proposed enhanced Optimized Link State Routing protocol, detection of wormhole link is based on frequency of use parameter of each node. If at all any node proves to be a part of route contains wormhole tunnel then no packet can be further send through that node. Wormhole attackers pretend two far away nodes as neighbor but they are multi hop away to each other. Generally the attackers aim is to pass maximum traffic through wormhole tunnel so that they can access drop or modify it. But in wormhole attack if attacker don't access, drop or modify the packet it can disrupts the whole network topology. As a result of wormhole attack all packets leads to wormhole tunnel. This factor is used to detect wormhole attack in our scheme. This modified Topology set also contain one field for frequent appearance count. When any node is used for routing its corresponding frequent appearance count is increment by one.

The proposed routing protocol is applicable to following:

- Mobile ad hoc network specially large and dense heterogeneous wireless networks.

- Wireless network where traffic is random between a large set of nodes.
- Wireless networks where the communicating peer changes over time.
- Wireless networks where immediate secure route required without delay.

IV. CONCLUSION

This work propose comparison study of optimized link state routing protocol and proposed secure optimized link state routing protocol in the presence of wormhole attack and to conclude different security issues of mobile ad hoc networks as well as implementation and detection of wormhole attack. The general issues, basic architecture, application area and routing protocols in Mobile Ad hoc Network are discussed.

V. REFERENCE:

[1] Jain M. and Kandwal H."A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks" in International Conference on Advances in Computing, Control, and Telecommunication Technologies,2009

[2] Y.C. Hu, A. Perrig and D. B. Johnson "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*" In IEEE INFOCOM, vol.3, pp. 1976 – 1986, (Apr.2003).

[3] Azeddine Attir et.al."Logical Wormhole Prevention in Optimized Link State Routing Protocol" in the IEEE GLOBECOM 2007 proceedings.

[9] Guoxing Zhan, Weisong Shi, and Julia Deng, 2012 "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" *IEEE Transactions on Dependable and Secure Computing*, Volume 9, Issue 2, pp.184-197

[10] S. Capkun, L. Buttyan, and J. Hubaux, *"SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks,"* In Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), Fairfax, USA, Oct.(2003).

[11] 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.

[12]Dang Quan Nguyen et.al."A Simple and Efficient Detection of Wormhole Attacks" 978-2-9532443-0-4 © 2008 ESRGroups France

[13] Saurabh Gupta et.al." WHOP: Wormhole Attack Detection Protocol using Hound Packet" in International Conference on Innovations in Information Technology(2011)

[14] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc on-demand distance vector (AODV) routing", IETF RFC 3561, July 2003.

[15] Ritu Malik, Meenakshi Mittal, Isha Batra and Chander Kiran, "Article: Wireless Mesh Networks (WMN)", International Journal of Computer Applications 1(23):66–74, February 2010.

[16] Theodore S. Rappaport, "Wireless Communications, Principles and Practice", 2nd edition, pp.643, 2003.

[17] Royer, E.M. Perkins, C.E.,"An Implementation Study of AODV Routing Protocol", In Wireless Communications and Networking Conference, 2000. WCNC, pages 1003 – 1008 vol.3 IEEE 2000.

[18] Yaling Yang, Jun Wang,"Design Guidelines for Routing Metrics in Multihop Wireless Networks", In IEEE INFOCOM - The 27th Conference on Computer Communications, pages 1615-1623. IEEE. 2008.