“A Review Paper of Dropping the Consequence of Jellyfish Attack in MANET using AODV and OLSR Routing protocol”

Teg Singh Ph.D. scholar[1], Dr. Rajesh Chauhan[2]
[1]*Career point University Kota,*
[2]*Associate Prof. HPU*

Abstract**—** Now a day, Ad-hoc network has become an invisible part for communication for mobile devices. A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes dynamically forming a network topology without the use of any existing network infrastructure. Routing is the process which transmitting the data packets from a source node to a given destination. The classes of routing protocols are proactive (table driven), reactive (on demand) and hybrid. In this paper we discuss an optimized link state routing protocol, named OLSR and Ad-hoc on demand distance vector routing protocol, named AODV for mobile wireless networks. The most efficient reactive protocol is AODV routing protocol. OLSR protocol is based on the link state algorithm and is a proactive in nature. OLSR is an optimization over a pure link state protocol as it compacts the size of information sent in the messages, and reduces the number of retransmission to flood this message in entire network.

Keyword- Routing protocol, Ad hoc network, Proactive and reactive routing protocols, AODV & OLSR.

I. INTRODUCTION

The different types of networks available today are Wired and Wireless networks. Wired are differentiated from wireless as being wired from point to point.

1.1 WIRED NETWROKS

These networks are generally connected with the help of wires and cables. Generally the cables being used in this type of networks are CAT5 or CAT6 cables. The connection is usually established with the help of physical devices like Switches and Hubs in between to increase the strength of the connection. These networks are usually more efficient, less expensive and much faster than wireless networks. Once the connection is set there is a very little chance of getting disconnected.

1.2 WIRELESS NETWORK

A significant factor in the development of a nation is a decent correspondence foundation and perceives how remote systems have a significant task to carry out in the improvement of a nation like India. Remote systems are normal, both for associations and people. Numerous PCs remote cards pre-introduced. The capacity to enter a system while versatile has incredible advantages. In any case, remote systems administration has numerous security issues. Programmers have discovered remote systems moderately simple to break into, and even utilize remote innovation to split into wired systems. Thus, it's significant that endeavors characterize successful remote security arrangements that guard against unapproved access to significant assets. Remote security is the avoidance of unapproved access or harm to PCs utilizing remote systems. Remote Interruption Anticipation Frameworks are usually used to uphold remote security approaches. The dangers to clients of remote innovation have expanded as the administration has gotten increasingly well known. There were generally not many risks when remote innovation was first presented. Saltines had not yet had the opportunity to lock on to the new innovation and remote was not ordinarily found in the work place. Notwithstanding, there are an incredible number of security dangers related with the present remote conventions and encryption techniques, and in the inconsiderateness and obliviousness that exists at the client and corporate IT level. Splitting strategies have gotten substantially more complex and inventive with remote. Breaking has likewise become a lot simpler and increasingly open with simple to-utilize Windows or Linux-put together devices being made accessible with respect to the web at no charge. We will investigate with respect to remote security, Dangers to remote security, Remote Interruption Counteraction Frameworks, Remote Security Best Practices and attempt to discover some recommendable Security Setups in down to earth.

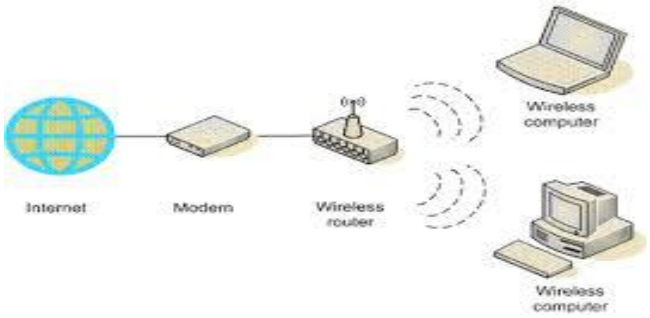

Fig 1: Wireless Communication

II. MANET

In the present quick and quickly developing universe of advancements, an ever increasing number of organizations comprehend the benefits of utilization of PC organizing. Contingent upon the association's size and assets it may be a little LAN containing just two or three dozen PCs; anyway in huge partnerships the systems can develop to huge and complex blend of PCs and servers.

The fast innovation headway has incited incredible development in cell phones associated with the Web. Versatile specially appointed system is the one comprising of an assortment of wireless mobile nodes (MNs) sharing a remote channel with no incorporated control or built up correspondence spine. The hubs themselves are liable for creation, activity, upkeep of the system and furthermore self-arrange to shape a system over radio connections. As a rule, these hubs go about as both end frameworks and switches simultaneously. The objective of MANETs is to expand versatility into the territory of self-sufficient, portable and remote areas, where a lot of hubs structure the system directing foundation in a specially appointed manner. Directing conventions should perform four significant elements of assurance of system topology, keeping up organize network, transmission planning and channel task, and bundle steering. Directing conventions in MANETs were created dependent on the structure objectives of insignificant control overhead, negligible preparing overhead, multi jump steering capacity, dynamic topology support and circle counteraction.

Versatile remote system is the framework less portable system, normally known as a specially appointed system. Framework less systems has no fixed switches; all hubs are fit for development and can be associated powerfully in a discretionary way. Hubs of these systems work as switches which find and keep up courses to different hubs in the system. A Versatile Specially appointed System is an assortment of free portable hubs that can convey to one another by means of radio waves. The portable hubs that are in radio scope of one another can legitimately convey, though others need the guide of moderate hubs to course their parcels. Every one of the hubs has a remote interface to speak with one another. These systems are completely disseminated, and can work at wherever without the assistance of any fixed framework as passageways or base stations.

A mobile ad-hoc network (MANET) is a self-arranging system of versatile switches (and related hosts) associated by remote connections - the association of which structure an arbitrary topology. The switches are allowed to move arbitrarily and sort out themselves aimlessly; along these lines, the system's remote topology may change quickly and erratically. Such a system may work in autonomously style, or might be associated with the bigger Web. Negligible arrangement and fast organization make specially appointed systems reasonable for crisis circumstances like normal or human initiated fiascos, military clashes, and crisis clinical circumstances and so forth. In addition, the system can be stretched out to wherever or working without the requirement for a wired association.

One of the particular highlights of MANET is, every hub must have the option to go about as a switch to discover the ideal way to advance a parcel. As hubs might be portable, entering and leaving the system.

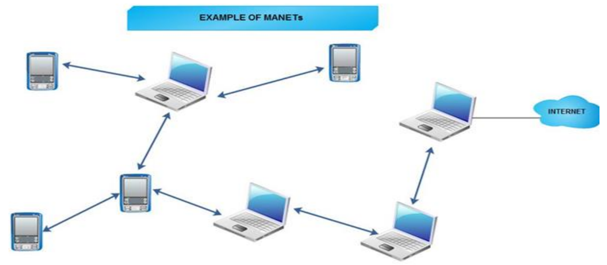

Fig 2 MANET Network

The topology of the system will change consistently Security is a basic prerequisite in mobile ad hoc network (MANETs). There are five significant security objectives that should be tended to so as to keep up a solid and secure specially appointed system condition. They are primarily:

1. Confidentiality: Insurance of any data from being presented to unintended elements. In specially appointed systems this is increasingly hard to accomplish in light of the fact that intermediates hubs get the bundles for different beneficiaries, so they can without much of a stretch listen in the data being steered.

2. Availability: Administrations ought to be accessible at whatever point required. There ought to be a confirmation of survivability in spite of a Disavowal of Administration (DOS) assault. On physical and media get to control layer aggressor can utilize sticking systems to meddle with correspondence on physical channel. On arrange layer the aggressor can disturb the directing convention. On higher layers, the aggressor could cut down elevated level administrations.

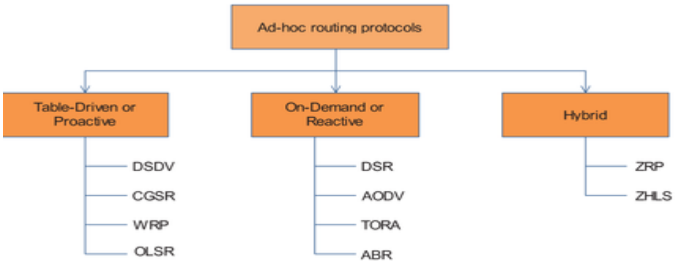

Fig 3 MANET Routing Protocol

Routing protocol characterize a lot of rules which oversees the excursion of message parcels from source to goal in a system. There are three sorts of directing conventions.

III. OLSR

The information right now the Propelled Association State Show is taken from its RFC 3561 [2]. Optimized Link State Protocol (OLSR) is a proactive steering convention, so the courses are for each situation rapidly available when required. OLSR is an improvement variation of an unadulterated association state show. So the topological changes cause the flooding of the topological information to each and every available host in the framework. To reduce the possible overhead in the framework show uses Multipoint Relays (MPR). The chance of MPR is to diminish flooding of imparts by diminishing a comparative convey in specific territories in the framework, more bits of knowledge concerning MPR can be found later at this moment. Another exercise is to give the briefest way. The diminishing the time between times for the control messages transmission can bring more prominent reactivity. OLSR utilizes two sorts of the control messages: Hi and Topology Control (TC). There is likewise Multiple Interface Declaration (MID) messages which are utilized for illuminating other host that the reporting host can have different OLSR interface addresses. The MID message is communicated all through the whole system just by MPRs. There is likewise a "Host and Network Association"(HNA) message which gives the outside directing data by giving the opportunities for steering to the outer locations. The HNA message gives data about the system and the net mask addresses, so that OLSR host can consider that the declaring host can go about as a door to the reporting set of addresses. The HNA is considered as a summed up adaptation of the TC message with just distinction that the TC message can illuminate about course dropping while HNA message data is expelled simply after termination time. The MID and HNA messages are not clarified in more subtleties right now, additional data concerning these messages can be found in [2]. Multipoint Hand-off center points furthermore picked with the help of Greetings Message [4]. Right when center points establish a connection with its closer centers than the essential bounce neighbor sends Greetings Message to its further nearer center and tells the sender that they have further centers which he needs to retransmit the data. Sender center points select those center points as a Multipoint Move center.

IV. AODV

It is a receptive improvement of the DSDV convention. AODV limits the quantity of course communicates by making courses on-request [19], rather than keeping up a total rundown of courses as in the DSDV calculation. Like DSR, it has on-request procedure of finding courses, the course demand is then forward by the source to the neighbors, etc, until either the goal or a middle hub with a new course to the goal, are found.

V. COMPARISON OF ROUTING PROTOCOL

Parameters	Reactive Protocol	Proactive Protocol	Hybrid protocol
Routing Philosophy	Flat	Flat/Hierarchical	Hierarchical
Routing Scheme	On Demand	Table Driven	Combination of both
Routing overhead	Low	High	Medium
Latency	High due to flooding	Low due to routing tables	Inside zone low outside similar to Reactive protocols
Scalability Level	Not suitable for large networks	Low	Designed for large networks
Availability of routing information	Available when required	Available when required	Combination of both
Periodic Updates	Not needed as route available on demand	Yes. Whenever the topology of the network changes	Yes needed inside the zone
Storage Capacity	Low generally Depends upon the number of routes	High ,due to the routing tables	Depends on the size of Zone, inside the Zone sometimes high as proactive protocol
Mobility Support	Route maintenance	Periodical Updates	Combination of both

VI. NETWORK ATTACKS

One of the two kinds A) gathers information in travel, without the interference of correspondence between approved gadgets. B) Enter a remote system through a security opening. A detached assault doesn't require complex strategies or apparatuses so as to listen in and gather information.

6.1 FLOODING ATTACKS

In flooding assault, aggressor debilitates the system assets, for example, data transmission and to devour a hub's assets, for example, computational and battery power or to disturb the directing activities to cause serious corruption in organize execution.

6.2 BLACK HOLE ATTACK

Course revelation process in AODV is helpless against the dark gap assault. The instrument, that is, any middle of the road hub may react to the RREQ message in the event that it has a new enough course, conceived to lessen steering delay, is utilized by the vindictive hub to bargain the framework. Right now, a vindictive hub tunes in to a course demand parcel in the system, it reacts with the case of having the most brief and the freshest course to the goal hub regardless of whether no such course exists. Thus, the vindictive hub effectively misroute organize traffic to it and afterward drop the bundles brief to it.

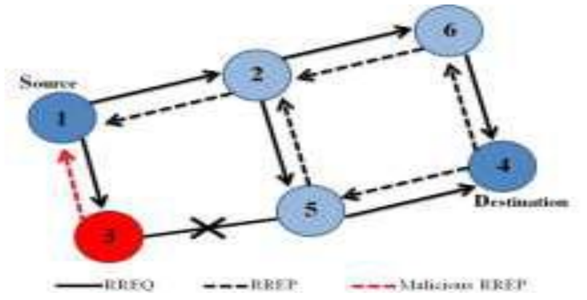

Fig: 4 Black Hole attack

6.3 GRAY WHOLE ATTACK

This attack is otherwise called directing bad conduct assault which prompts dropping of messages. The dark gap assault has two stages. Dim gap assault has two stages. In the primary stage the hub promote itself as having a legitimate course to goal while in second stage, hubs drops caught bundles with a specific likelihood. Right now assault the assailant deludes the system by affirming to advance the parcels in the system. When it gets the parcels from the neighbouring hub, the assailant falls the bundles; this attack goes under the class of dynamic assault. First and foremost the assailant hubs acts normally and answer genuine RREP messages to the hubs that began RREQ messages. At the point when it gets the bundles it begins dropping the parcels and dispatch Denial of Service (DoS) assault. The pernicious exercises of dark opening assault might be unique in relation to time to time. It might drops bundles while sending them in the system. In some other dim opening assaults the assailant hub carries on noxiously for the time until the bundles are dropped and afterward change to their ordinary conduct. Due this conduct it is extremely dubious for the system to make sense of such sort of assault.

6.4 WORMHOLE ATTACK

An aggressor records bundles at one area in the system and passages them to another area [1][2][3][4]. Steering can be upset when directing control messages are burrowed. This passage between two intriguing aggressors is alluded as a wormhole [1][2][3][4].Wormhole assaults are extreme dangers to MANET steering conventions. Wormholes are difficult to distinguish on the grounds that the way that is utilized to pass on data is generally not part of the genuine system. Wormholes are risky in light of the fact that they can doharm without knowing the system [6].

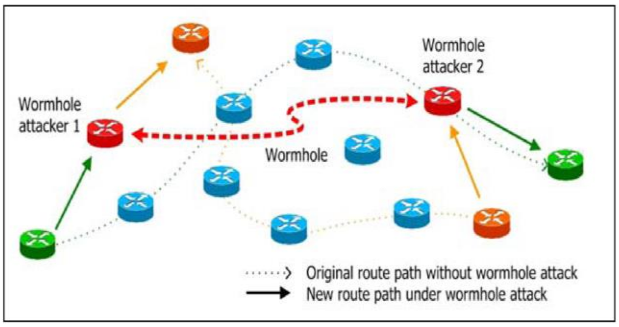
Wormhole attacker 2
Wormhole attacker 1
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

Fig: 5 Wormhole attack

For instance, when a wormhole assault is utilized against an on-request steering convention, for example, DSR or AODV the assault could forestall the disclosure of any courses other than through the wormhole[3][4][5][9].

6.5 JELLYFISH ATTACK

Jelly fish attack is one of the disavowals of administration assault and furthermore a kind of inactive assault which is hard to distinguish. It produces delay before the transmission and gathering of information parcels in the system. Applications, for example, HTTP, FTP and video conferencing are given by TCP and UDP. Jellyfish assault upsets the presentation of the two conventions. It is same as dark gap assault however the thing that matters is that the dark gap aggressor hub drops all the information parcels yet jellyfish assailant hub produces delay during sending bundles. Jellyfish assaults are focused against shut circle streams. TCP has notable vulnerabilities to deferral, drop and miss-request the parcels. Because of this, hubs can change the arrangement of the parcels additionally drop a portion of the information bundles. The jellyfish assailant hubs completely obey convention rules; henceforth this assault is called as latent assault [3]. Jellyfish assaults are focused against shut circle streams. The objective of jellyfish hub is to reduce the great put, which can be accomplished by dropping some of bundles. At the point when a malignant hubs dispatches sending dismissal assaults it additionally may conform to all directing methods.[10] The Jellyfish assault is one of those sorts. A vindictive hub propelling Jellyfish assaults may keep dynamic in both course finding and bundle Manjot Kaur et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April-2014, pg. 199-203 2014, IJCSMC All Rights Reserved 202 sending so as to keep it from discovery and analysis, yet the noxious hub can assault the traffic by means of itself by reordering bundles, dropping parcels occasionally, or expanding butterflies. [11] The Jellyfish assault is particularly unsafe to TCP traffic in that agreeable hubs can barely separate these assaults from the system clog. Reference likewise depicted that vindictive hubs may even maltreatment directional radio wire and dynamic force procedures to maintain a strategic distance from upstream hubs to distinguish their mischievous activities of dropping bundles. This assault for the most part targets shut circle streams in that capacity streams react to arrange conditions like parcel misfortune and bundle delay. It focuses on TCP's blockage control component. The fundamental objective of the Jellyfish hubs is to diminish the great put of the considerable number of streams to approach zero by either reordering the parcels or dropping a little portion of bundles. [4] These sending instruments are variations of Jellyfish attack.

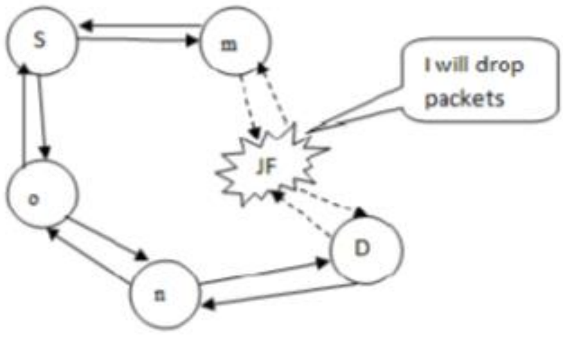

Fig: 6 Jellyfish Attack

As shown in Figure 1.7, node JF is a Jellyfish, and node S starts to communicate with node D after a path via the Jellyfish node is established. Then the Denial of service attacks launched by node JF will cause packet loss and break off the communications between nodes S and D eventually. [3].

TABLE 1: Comparative analysis of AODV, DSR and OLSR

S. No	Parameters	AODV	DSR	OLSR
1.	Routing Type	Reactive	Reactive	Proactive
2.	Route Selection	Shortest & update path	Shortest & update path	Shortest route
3.	Multiple Route	No	Yes	Yes
4.	Routing structure	Flat structure	Flat structure	Flat structure
5.	Suited for	Well suited for large network	Well suited for small network	Well suited for large network
6.	Multicasting	Yes	No	Yes
7.	Congestion Handling	Yes	No	Yes
8.	Route maintain in	Route table	Route cache	Routing table
9.	Updates transmitted to	Source	Source	Neighbor
10.	QoS support	No	No	Yes
11	Periodic Broadcast	Yes	Yes	Yes

VII. CONCLUSION

MANET is an independent system of mobile nodes connected by wireless links that perform towards the secure and efficient routing protocols. OLSR protocol is a preemptive protocol for low latency route determination in MANETs. For mobile wireless network, the performance of a routing protocol is coupled with many factors, like the choice of physical technology, link layer etc. OLSR is protocol is proactive or table driven in nature. Due to the popularity of the AODV protocol a number of variations and improvements on the core protocol have been proposed by researchers to address specific issues with the protocol.

VIII. REFERENCES

[1] S. Corson and J. Macker (1999), “Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations,” IETF RFC 2501.

[2] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications ISO/IEC8802- 11; ANSI/IEEE Standard 802.11, Aug. 1999.

[3] Bluetooth Core Specification, v1.2, Nov. 2003.

[4] E. Perkins and P. Bhagwat (1994), “Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers”, Proceedings of ACM SIGCOMM 94, pp. 34–244.

[5] Tsu-Wei Chen and M. Gerla (1998), "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks" Proceedings of International Computing Conference IEEE ICC.

[6] S. Murthy and J. J. Garcia-Luna-Aceves (1996), "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. Journal, Special Issue on Routing in Mobile Communication Networks, Pp.183-97.

[7] C. Perkins, E. B. Royer, S. Das(2003), “Ad hoc On- Demand Distance Vector (AODV) Routing - Internet Draft”, RFC 3561, IETF Network Working Group.

[8] B. Johnson and D. A. Maltz (1996), "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T.Imielinski and H. Korth, Eds., pp. 152-81.

[9] Park and S. Corson (1998), “Temporally Ordered Routing Algorithm (TORA) Version 1, Functional Specification IETF Internet draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt.

[10]Thakur Ankur, Department of Computer Science Engineering RIMT MandiGobindgarh, India (Punjab), “Quoted in International Journal of innovation in Engineering and Technology (IJIET)”.

[11]Kumar Sandeep, Sangeeta, Kumar Pramod (2014),”A Review on Gray Hole Attack in MANETs”, ISSN: 2277 128X International Journal of Advanced Research in Volume 4, Issue 9, pp 70-75.

Teg Singh, Assistant Professor in the Department of Computer Science ,BCA & PGDCA working in Govt. College Bilaspur and having an experience of 12 years in Teaching. I m pursuing Ph.D in CSE from Career Point University Kota Rajsthan under the guidance of **Dr. Rajesh Chauhan,** Assistant Professor, UIIT HPU Shimla.