International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

Mobile Ad Hoc Networks: An Overview

Dr. Gaurav Sharma
Associate Professor,
Deptt. of Computer Science & Engg.,
JMIT Radaur, Yamunanagar, (Haryana), India

Surbhi Dhiman
M. Tech Scholar,
Deptt. of Computer Science & Engg.,
JMIT Radaur, Yamunanagar, (Haryana), India

***Abstract*-Mobile Ad-Hoc Network (MANET) is an infrastructure less wireless network of mobile nodes (Smart phones, Laptops, iPads, PDAs etc.) that self-configure to reconstruct their topology and route table information for the exchange of data packets. In MANET there is no central administration framework for design obligation. Every versatile node uninhibitedly moves, enter and detach with no pre information. The wireless links in this network are highly unsecure and can go down frequently due to mobility of nodes, interference and less infrastructure. In this research paper an attempt has been made to discuss the characteristics, limitations and comparative analysis of routing protocols in MANETS.**

Keywords- MANETs, Ad Hoc Network, Attacks, Routing Protocols, Survey, Review

1. INTRODUCTION

MANET is a kind of wireless network where one can achieve wireless communication in a limited area network. An Ad Hoc Network is the best example of MANET where one does not have any access point or device in between the group of communication devices. It can be any wireless device like Mobile, Printer or any other wireless media. Mobility in Ad Hoc Networks introduces portability but on the other hand mobility is not so easy to achieve and work within wireless network causes traffic problem, link disjoined and breakages due to the dynamic mobility. Each node in the network acts both as a host and as a router at the same time to do both transmission and reception in the network. As the nodes keep moving in the network, the topology of the network changes frequently and it is not predictable. Whenever a node wants to communicate with another node which is out of its radio range, the intermediate nodes in the network are needed which is known as the multi-hop communication. Some of the nodes in the MANET are operated on battery and also their energy is very limited. So, running the normal operations of a MANET by conserving energy depends upon the design and a better implementation of the MANET. Along with this some other challenges for a MANET are bandwidth, quality of service, network topology and security. There are a wide range of applications for the MANET, ranging fromclassroom/meeting room applications, data collection networks and even in military applications.

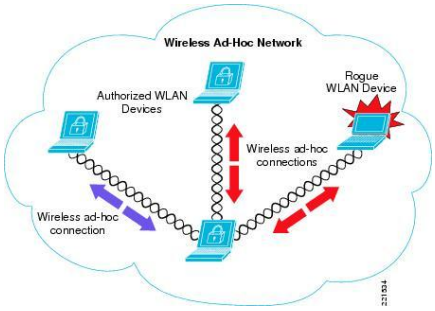

Fig. 1 Mobile Ad Hoc Network

2. LITERATURE SURVEY

The routing problems in ad hoc network have gained attention among the researchers, and many routing protocols for ad hoc network have been proposed [1, 11, 12, 16].

Ashwani Kush and Sunil Taneja have described the routing protocols in mobile ad hoc networks. They have given an overview of the DSR, AODV and TORA protocols presenting their characteristics, functionality, benefits and limitations[1].V. Park and M.S. Corson emphasized on a conceptual description of the protocol Temporally-Ordered Routing Algorithm (TORA) which is a highly adaptive distributed routing algorithm and tailored for operation in a mobile networking environment. It is one of a family of "link-reversal" algorithms[2]. The basic routing mechanism of TORA is neither a distance-vector nor a link-state routing

C. Perkins et al. presented an overview of Ad Hoc on Demand Distance Vector (AODV) routing protocol which is a variation of Destination-Sequenced Distance-Vector (DSDV) routing protocol and collectively based on DSDV and DSR.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

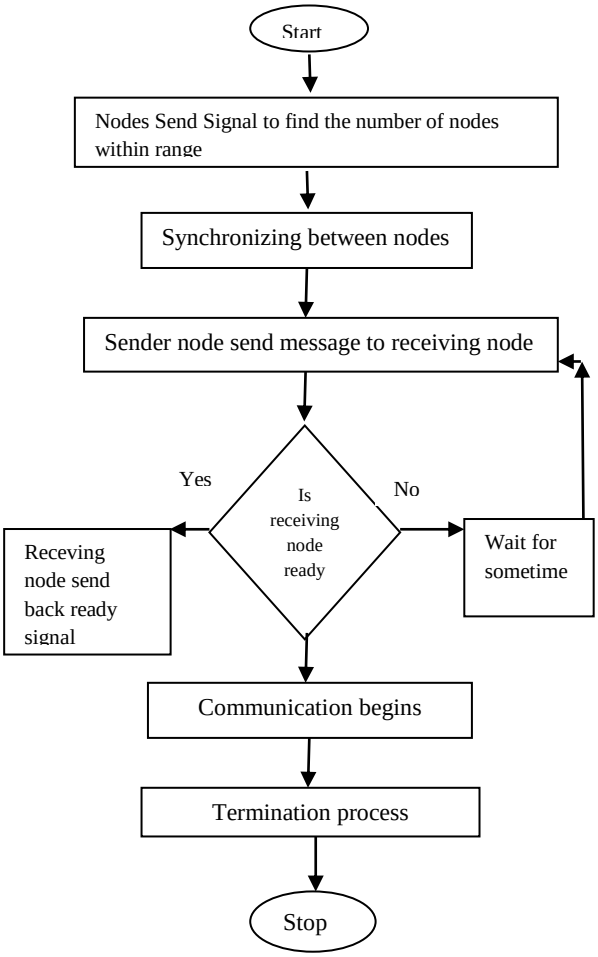

Fig 2. General Working of MANETs

It does not maintain routes from every node to every other node in the network rather they are discovered as and when needed & are maintained only as long as they are required [3]. S. Singh et al. and Lin proposed a routing algorithm based on minimizing the amount of power required to transfer a packet from source to destination [4, 5].

Holland and Vaidya studied the behavior of TCP in ad hoc networks, using DSR as a routing protocol. Their work added explicit interaction between TCP and the Route Discovery and Route Maintenance mechanisms that allow TCP to correctly react to a route failure rather than treating it as network congestion [6].

For quality assurance different strategies attempting to manage limited resources like bandwidth, computation power, memory and battery in ad hoc wireless networks have been developed.

Jeffery P. Hansen et al. explained an approach for satisfying application-specific Quality of Service (QoS) expectations on ad hoc wireless networks where available bandwidth fluctuates. The proposed algorithm, D-Q-RAM (Distributed QoS Resource Allocation Model) generates a distributed optimization heuristic that results in near optimal adaptation without the need to estimate, or predict available bandwidth at any moment in time [7].

Stephen F. Bush proposed a metric that couples network topological rate of change with the ability of a generic service to move itself to an optimal location. The metric proposed a fundamental tradeoff among adaptation (changed service location), performance, and network ability to tune itself to a changing ad hoc network topology[8].

Swati Jaiswal et al. discussed the Quality of services(QoS) issues in mobile ad-hoc networks. QoS for a network is measured in terms of guaranteed amount of data transferred from one place to another in a given time slot. QoS support for Mobile Ad-hoc Networks is a challenging task due to dynamic topology & limited resources. The main purpose of QoS routing is to find a feasible path that has sufficient resources to satisfy the constraints[9].Goyal et al. analyzed the routing protocols for wireless ad hoc networks based on their performance. This is done theoretically as well as through simulation. They identified suitable routing protocols for use with WSN based on the limitations of the technology and proposed an enhanced protocol for WSN[10].

Neerja Khatri and Arvind Kumar evaluated the performance of AODV protocol in MANET with different network parameters using network simulator. They presented information related to AODV protocol and modifications done to it to improve its performance [11]. Nitin Goyal and Alka Gaba provided a universal thought of routing protocols and also brief indication over Location Based Routing Protocols.They concluded that a protocol is still required to deal with energy efficient issue. A number of protocols are there but still they have not considered energy efficient issue. Work is still left over in MANET to have efficient storage capacity, computation capability, and power[12].

Sina Shahabi et al. suggest a new algorithm which enhances the security of AODV routing protocol to encounter the black hole attacks. This algorithm tries to identify malicious nodes according to nodes behavior in an Ad Hoc network and remove them from routing. The proposed algorithm is simulated by NS2. The simulation results show some improvements in end-to-end delay and packet delivery rate in the suggested algorithm [13]. Sandeep Kumar Aroraet al. implemented Intrusion Detection System using NS-2 by modifying the original AODV protocol and removing the black hole node which drops the maximum packets. They also proposed a method of selecting the path of highest sequence number which is helpful in achieving the better Quality of Services (QoS). The scheme was conducted to analyze the performance of the IDS technique over existing techniques which revealed that the Packet Delivery Ratio is improved by 60% [14].Houda Moudni et al. simulated black hole, flooding and rushing attacks which are threats in AODV routing protocol to analyze their impacts on this protocol using NS-2 network simulator. They took into consideration the network size, nodes mobility,traffic load and the number of the attackers. They used packet delivery ratio, average end-to-end delay and throughput as performance evaluation metrics[15]

3. CHARACTERISTICS OF MOBILE AD HOC NETWORKS

The characteristics which MANETs have to achieve are self-configuration, peer-to-peer connection among hosts and dynamic multi-hop routing. Some basic characteristics [1] are as follows:-

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

In MANET, each node acts as both host and router. That is it is autonomous in behavior.

Multi-hop routing: When a source node and destination node is out of radio range, MANET find out various path through intermediate nodes which is in direct range of network this is multi-hop routing process.

Distributed Operation: For security, routing and host configuration, there is no centralized firewall and proposed topology is infrastructure less.

Dynamic Network Topology: The nodes can join or detach from the network anytime, making the network topology dynamic in nature.

Fluctuating Link Bandwidth: The effects of high bit error rate are more common in wireless communication.

Limited Energy Resources: Mobile nodes have less memory, power and light weight features. Wireless devices are battery powered therefore designing. Mechanisms used to reduce energy consumption are: (a) devices goes into sleep state when no sending and receiving of data (b) routing paths that minimize energy consumption, (c) develop communication and data delivery structures that minimize energy consumption and (d) reduce networking overhead.

4. VULNERABILITIES OF MOBILE AD HOC NETWORKS

Vulnerability is weakness in security system. A particular system may be vulnerable to unauthorized data manipulation as the system does not verify a user's identity before allowing data access. MANET is more vulnerable than any wired network. Some of the vulnerabilities of MANET are as follows:-

Lack of centralized management: MANET do not have a centralized monitor server. The absence of centralized management makes the detection of attacks quite difficult because it is not easy to monitor the traffic in a dynamic and large ad-hoc network.

Resource availability: Resource availability is a major issue in MANET. Having secure communication and protection against various threats and attacks, leads to development of various security schemes.

Scalability: Due to mobility of nodes, topology of ad-hoc network altersdynamically. So scalability is a major issue for security. Security mechanisms should be capable of handling large as well as small networks.

Dynamic topology: Dynamic topology and changing nodes membership may disturb the trust relationship among nodes. The trust is also disturbed when some nodes are detected as compromised. This dynamic behavior can be preserved with distributed and adaptive security mechanisms.

Power supply limitation: The nodes in ad-hoc network need to consider restricted power supply, which will cause several problems. A node in ad-hoc network may act in a selfish manner when it finds that there is only limited power supply.

Adversary inside the Network: The mobile nodes within the MANET can freely join and detach from the network. The nodes within network may behave maliciously. It is hard to detect about the malicious behavior of the node. Thus this attack is more dangerous than the external attack. These nodes are compromised nodes.

No predefined Boundary: In mobile ad- hoc networks, we cannot precisely define a physical boundary of the network. The attacks are eavesdropping, impersonation; tempering, replay and Denial of Service (DoS) attack [2].

5. APPLICATIONS OF MOBILE AD HOC NETWORKS

The Ad hoc system is not intended to be utilized where it is dependably reachable, as in 2G and 3G cell frameworks. Its primary qualities are heartiness of the system, the consistent connectively with nodes in the network area and the way that the system comprises of taking an interested node. Discussed below are several applications that can benefit from an Ad-hoc network.

Rescue operations: There are numerous circumstances where there is no infrastructure present, yet where it is important to build up a system. Circumstances like natural disaster, wars and emergency in immature nations, are case of this. Specially appointed systems are a vivid arrangement, since such systems can be conveyed rapidly and have no need of any framework.

Home networks: Today, numerous family units have few PCs in various rooms. Many people might want to connect these to each other. Regardless of the fact that there are a few available methods for associating them together, the specially appointed system is a simple and rich arrangement.

Games: This is an example of a completely commercial aspect of the ad hoc network. People can now play with the general population unintentionally inside the network area. This is an awesome approach to side interest in broad daylight zones as in trains, train stations or air terminals.

Military: It was the U.S Department of Defense that supported the principal exploration of specially appointed systems to empower parcel changing innovation to work without the confinement of an altered wired base. They did this with great reasons; the strength of the system is without examination. To disable the system an opponent must decimate a vast rate of the dynamic hubs. Since a standout amongst the most critical chore in a military battle is to keep order lines open, it is required that the military foundation has a considerable measure into growing specially appointed systems.

6. SECURITY ATTACKS IN MOBILE AD HOC NETWORKS

In MANET network there are security issues in almost each layer. [5]The main network-layer functions in MANET are ad hoc routing and data packet forwarding, which fulfill the functionality of delivering packets from the source to the destination. Following are the attacks in network layer:-

Spoofing: Malicious node acts as a valid node of that network and pretends as another node. Now this malicious node affects communication, sniffs and disturbs access rights [6] as shown in Figure 3.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

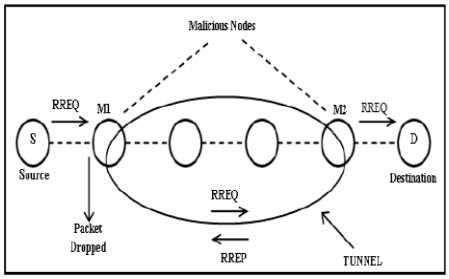

Fig. 3: Spoofing (Man in Middle) attack

Black hole Attack: In this attack, the malicious node captures the request from source and sends response to source behaving like destination node [7]. All the packets from source are consumed by malicious node are destroyed(figure 4).When source node wants to communicate to destination node; it starts the path discovery process. The malicious node captures request of source node, and immediately sends response to source. If reply from malicious node reaches first to the source then source node ignores all other reply messages from network and begin to send packet through malicious route node. As a result, all data packets are consumed or lost at malicious node.

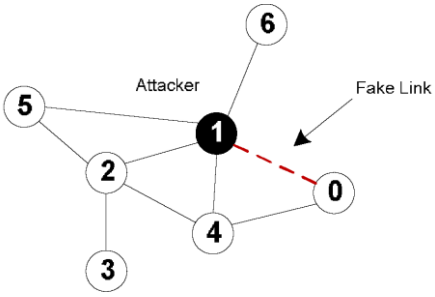

Fig. 4: Blackhole attack

Wormhole Attack: An attacker adds a new fake optimal path which is external shortest path between nodes.This shortest path acts as a tunnel between nodes and being a shortest path, it is selected as a new route by routing algorithms for data transmission[5] and [7]. In this way real transmission path is destroyed (Fig. 5). This tunnel is known as wormhole.

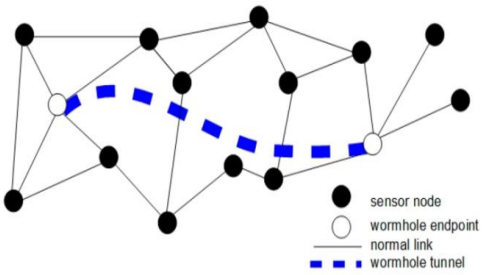

Fig. 5 Wormhole attack

Fabrication: Attacker in fabrication attack [8] adds new fake messages in the network between nodes to disrupt the routing process. These attacks are difficult toidentify because they act as valid routing scheme, especially fabricated routing error messages, which shows that a neighbor is out of network and not connected.

7. CHALLENGES IN MOBILE AD HOC NETWORKS

There are several issues in ad hoc networks that make them very complex to integrate with the existing global network. Generally the most prominent problems are the identification of mobile terminals and the correct routing of packets from and to each terminal while they are moving. The problems are addressed below :

Routing: Routing is a standout amongst the most captured issue to understand as specially appointed systems have a consistent network to different nodes in its neighborhood. Each node acts as a switch and advances each other's packages to empower data sharing between portable nodes.

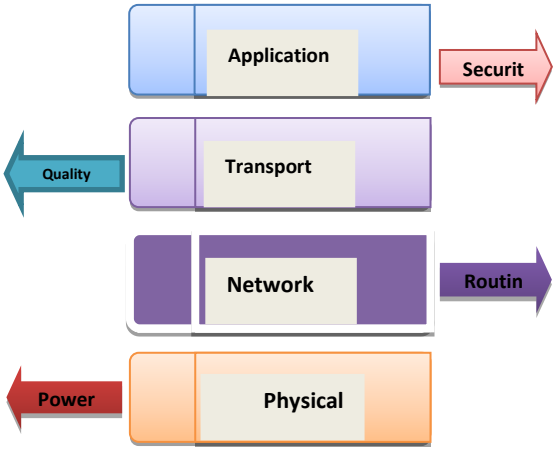

Fig 6. MANET Challenges

Security: A wireless link is much more vulnerable to attacks than awired link. The user cani nsert spurious information into routing packets and cause routing loops, longtime-outsand advertisements of false or old routing table updates. Security has several unsolved issues that are needed to be solved to make the adhoc networkagood solution.

Quality of Service: QoS is a troublesome assignment for the engineers, on the grounds that the topology of a specially appointed system will always show signs of change. Saving assets and maintaining a specific nature of administration, while the system condition continually changes, is exceptionally testing [3].

Power Control: Power control is another run of the mill objective in specially appointed system. Since each cell phone utilizing battery for force supply. Yet, it is for brief period. In cell phones power utilization rely upon various sort of directing conventions or steering strategies.

A. Proactive Routing Protocols

These algorithms maintain a route to the destination much like the traditional fixed networks. When the packet is to be transmitted it just picks up a route from the node cache and uses it. This causes the instant transmission of the first packet, but the nodes have to work hard in the background to establish routes, wasting precious radio resources.

One prominent protocol in the proactive class is the DSDV Protocol (Destination Sequenced Distance Vector). Proactive routing protocols (also called Table-driven routing protocols) attempts to maintainconsistent, up todate routing information between each node in the network.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

These protocols require in each node to maintain one or more tables to store routing information, and responding to changes in network by propagating route updates throughout the network to maintain a consistent network view.

B. Reactive Routing Protocols

Reactive routing protocols, also called on demand routing protocols, create and maintain routes only in an as needed basis, unlike proactive protocols where routes are maintained to all potential destinations. When a route is needed, a global route discovery procedure is initiated to find the path for the specific information that has not been cached. The route discovery is done by employing classical flooding mechanism.

The three prominent protocols in the reactive class are DSR (Dynamic Source Routing), AODV (Ad hoc on Demand Distance Vector Routing) and TORA (Temporary Ordered Routing Algorithm).

An approach that is different from table-driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node.

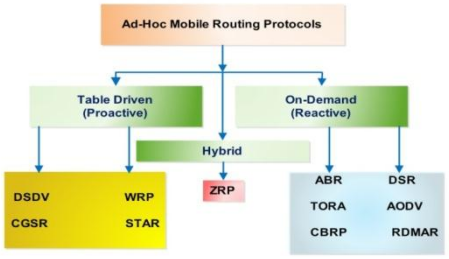

Fig 7. Types of Routing Protocols

7.1 Ad Hoc on Demand Distance Vector (AODV)

AODV belongs to the class of Distance Vector Routing Protocols (DV). In DV every node knows its neighbours and the costs to reach them. Ad hoc On Demand Distance Vector (AODV) is a reactive routing protocol that initiates a route discovery process only when it has data packets to forward and does not have any route path towards the destination node, that is, route discovery in AODV is on-demand. AODV is composed of three mechanisms: Route Discovery process, Route message generation and Route maintenance. The important feature of AODV is whenever a route is available from source to destination; it does not add any overhead to the data packets. However, route discovery process is only initiated when routes are not used or they expired and discarded. This reduces the effects of stale routes and the need for route maintenance for free routes. Another distinguishing feature of AODV is its ability to provide unicast, multicast and broadcast communication. AODV uses a broadcast route discovery algorithm and then the unicast route reply message.

Advantages:-

1. Reduced overhead.

2. Lower setup delay

Disadvantages:-

1. Periodic updates.

2. Inconsistent routes.

7.2 Destination Sequenced Distance Vector Routing(DSDV):

Destination Sequenced Distance Vector (DSDV) routing protocol is a variant of distance vector routing method in which the mobile nodes cooperate among themselves to form an Ad Hoc network. DSDV is based on RIP (Routing Information Protocol), used for Intra-Domain routing in Internet. DSDV requires each node in the network to maintain complete list of route information to reach each node in the Ad Hoc network. In DSDV, each node uses a Sequence Number, which is a counter that can be incremented only by that node. Routing information is propagated using broadcast or multicasting the messages periodically or triggered when a change in topology occurs. DSDV uses only bi-directional links for routing as it is based on Distance Vector Routing. So in DSDV, each node does not insert information into its Routing tablereceived from other neighbors unless the node is sure that the other node can listen to its advertisements.In DSDV, each node maintains a routing table and advertises this information to each of its neighbors periodically or immediately when there is a change in the topology. The routing data packet sent periodically by anode contains a new Sequence numberand the following information for each of the other mobile stations:

1.The Destination address

2.The number of hope required to reach the Destination

3.The Sequence Number of the Destination received regarding the destination.

A node upon receiving a new routing information packet from its neighboring node compares it with the previous routing information packets and then updates its routing table depending on the sequence number and the metric of the entries. Any route with higher Sequence Number is always chosen regardless of the value of the metric. Routes with old Sequence Numbers are discarded. In case of same sequence number as the existing route, a route with the least cost metric is chosen. Thus each node in DSDV maintains two routing tables, one used for forwarding the data packets and the other for advertising incremental routing packets.

Advantages:

1. Less delay in the path set up process

2. Adaptability to dynamic networks.

Disadvantages:

1. Single path from source to destination

2. High mobility rate

3. Not suitable for large size networks

7.3 Dynamic Source Routing Protocol (DSR)

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless networks of mobile nodes. It makes the network completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. DSR is reactive or on demand protocol. There is no periodic activity of any kind like hello messages in AODV. This protocol utilizes source routing (entire route is part of the header). It uses caches to store routes. The DSR protocol allows nodes to dynamically discover a source route across

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

network hopsto any destination in the ad hoc network. Each data packet sent carries in the header the complete, ordered list ofnodes through which the packet must travel, allowing packet routing to be loop-free and avoiding the need for up-to-date routing information in the intermediate nodes. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network.

Network nodes (computers)

Table 1. Comparison of various routing protocols

Protocol Property	DSDV	AODV	DSR	TORA	ZRP
Loop Free	Yes	Yes	Yes	Yes	Yes
Multiple Routes	No	No	Yes	Yes	No
Category	Proactive	Reactive	Both	Reactive	Proactive
Security	No	No	No	No	No
QOS Support	No	No	No	No	No
Power Efficiency	No	No	No	No	No

cooperate to forward packets for each other to allow communication over multiple “hops” between nodes not directly within wireless transmission range of one another.

Advantages:

1. Route is established only when it is required.
2. No need to keep routing table.
3. Reducing load.

Disadvantages:-

1. Higher delay.
2. The route maintenance.
3. Not scalable to large networks.
4. Requires more processing resources.

7.4 Temporally Ordered Routing Algorithm (TORA)

Temporally Ordered Routing Algorithm (TORA) is an efficient, adaptive and scalable distributed routing algorithm based on link reversal. TORA is designed for highly dynamic mobile, multi-hop wireless AdHoc networks. It has a unique feature of maintaining multi routes to destination so that topological alterations do not need any reaction at all. The protocol reacts only when all routes to the destination are lost.

The protocol has three basic functions: Route creation, Route maintenance and Route erasure.

Route creation: - When a node needs a route to destination, it initiates route creation where query packets are broadcasted to search for possible routes to the destination.

Route maintenance: - The availability of many paths is a result of how TORA models the entire network as a directed acyclic graph (DAG) rooted at the destination. Route maintenance occurs when a node losses all of its outgoing links. The node sends an update packet which reverses the links to all its neighboring nodes. The route maintenance function of TORA is the main problem as this function produces a large amount of routing overhead. It causes the network to be congested thus preventing data packets from reaching their destinations.

Route erasure:- In the case when a node is in a network partition without a route to the destination, route erasure is initiated. Route erasure is performed by flooding clear packets throughout the network. When a node receives a clear packet, it sets the links to its neighbors as unassigned. The clear packets distribute through the network and delete all routes to that unreachable node.

Advantages:-

1. Multiple paths created.
2. Communication overhead and bandwidth utilization is minimized.

Disadvantages:-

1. Routing overheads.
2. Depends on synchronized clocks among nodes.

7.5 Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) is a prototype routing protocol. ZRP is formed by two sub protocols, the Intra zone Routing Protocol (IARP) and the Inter zone Routing Protocol (IERP). IARP is a limited scope proactive routing protocol which improves the performance of existing reactive routing protocols. It relies on the service of a neighbor discovery protocol (NDP) to provide neighbor information. IARP may use a scheme based on the time-to-live (TTL) field in IP packets to control the zone range. IERP is the reactive routing component of ZRP. This scheme is responsible for finding a global path. When global queries are needed, the routing zone based broadcast service is used to efficiently guide route queries outwards, rather than blindly relaying queries from neighbor to neighbor. ZRP combines the advantages of reactive and proactive routing protocols.

Advantages:

1. Reduces the control overhead
2. Eliminates the delay for routing

Disadvantage:

1. Lack of route optimization

8. CONCLUSION

Mobile ad hoc networks are used in military operations, emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. In this paper we tried to inspect the introduction, characteristics and various attacks relating to mobile ad hoc networks. Firstly we briefly introduced the characteristics and analysis of various routing protocols of MANETS. The existing characteristics have made it necessary to find some effective security solutions and protect the MANET’s from all kind of security risks.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

REFERENCES

[1] Ashwani Kush and Sunil Taneja,"A Survey of Routing Protocols in Mobile Ad HocNetworks", International Journal of Innovation, Management and Technology, ISSN: 2010-0248, Vol. 1, No. 3, August 2010.

[2] V. Park and M.S. Corson,"A Highly DistributedRouting Algorithm for Mobile Wireless Networks," Proc. OfIEEE INFOCOM 97,Kobe, Japan, April 1997.

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

[4] S. Singh, M. Woo, C.S. Raghavendra, "Power AwareRouting in Mobile ad hoc networks", Proceedings of ACM Mobicom 98, Dallas, October, 1998.

[5] S. Lindsay, K. Sivalingam and C. S. Raghvendra, "Poweraware routing and MAC protocols for wireless andmobile networks", Wiley handbook on Wireless Networks and Mobile Computing; Ed., John Wiley &Sons, 2001.

[6] Galvin Holland and NitinVaidya, "Analysis of TCP Performance over Mobile Ad HocNetworks. In Proceedings of the Fifth International Conference on Mobile Computingand Networking (MobiCom'99), pages 219–230. ACM, August 1999.

[7] Jeffery P. Hansen, Scott Hissam, Daniel Plakosh and Lutz Wrage, "Adaptive Quality of Service in Ad Hoc Wireless Networks" IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks,2012.

[8] Stephen F. Bush, "A Simple Metric for Ad Hoc Network Adaptation" IEEE journal on selected areas in communications, vol. 23, no. 12, December 2005.

[9] Swati Jaiswal, SatyaPrakash, Neeraj Gupta, DevendraRewadikar,"Performance Optimization in Ad-hoc Networks", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 2,2008.

[10] Tauja Khurana, Sukhvir Singh, Nitin Goyal, "An Evaluation of Ad-hoc Routing Protocols for Wireless Sensor Networks", International Journal of Advanced Research in Electronics and Communication Engineering, Vol. 1, No. 1, July 2012.

[11] Neerja Khatri, Arvind Kumar, "Analysing Performance of AODV in MANET: A SURVEY", International Journal of Scientific and Engineering Research, 3, Issue 6, June 2012.

[12] Nitin Goyal, Alka Gaba, "A review over MANET- Issues and Challenges", International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471, Vol. 2, Issue 4, April-2013.

[13] Sina Shahabi, Mahdieh Ghazvini and Mehdi Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack", DOI 10.1007/s11276-015-1032-y, Wireless Network, Springer Science, 2015.

[14] Sandeep Kumar Arora, Shivani Vijan , Gurjot Singh Gaba, "Detection and Analysis of Black Hole Attack using IDS", Journal of Science and Technology, Vol. 9, Issue 20, May 2016

[15] Houda Moudni, Mohamed Er rouidi, Hicham Mouncif, Benachir El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks", 2nd International Conference on Electrical and Information Technologies ICEIT, May 2016, Date Added to IEEE Xplore: 25 July 2016.

[16] Pratibha Kamboj and Nitin Goyal, "Survey of Various Keys Management Techniques in MANET", International Journal of Emerging Research in Management & Technology 4, no. 6 (2015).

(This work is licensed under a Creative Commons Attribution 4.0 International License.)