International Journal of Education and Science Research Review
E- ISSN 2348-6457
Volume-1, Issue-5 October- 2014 P- ISSN2349-1817
www.ijesrr.org Email- editor@ijesrr.org

A Survey on Mobile Ad Hoc Network

Rajib Biswas
Assistant Professor
Electronics & Telecommunication Engineering
Tripura Institute of Technology
Agartala, India

Kushal Dey, Gouri Das, Anjali Kumari , Santana Chakma
U.G. Student
Electronics & Telecommunication Engineering
Tripura Institute of Technology
Agartala, India

ABSTRACT
Mobile Ad-hoc network is a wireless, infrastructure less temporary network. The performance of mobile ad-hoc networks (MANET) is related to the efficiency of the routing protocols in adapting to frequently changing network topologies and link status. In this paper we present a survey on MANET (wireless). Various protocols used in MANET are discussed in this paper. Designing of such routing protocols is not simple. MANET has its own quality of service, which must be efficient. As MANET is a free space communication network it is frequently get attacked by the third party device. Security issue in MANET is highly required. For efficient data transmission it is necessary to protect the network, so that data loss during transmission will reduce.

Keywords— AODV, FQMM, MANET, OLSR, proactive, Qos, reactive,

I. INTRODUCTION
MANET is a collection of wireless mobile hosts forming a temporary network. It is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. In MANET the structure of the network changes dynamically which means each device in MANET is free to move independently in any direction. Each device in MANET is known as node. This nodes act as routers that route data to or from other nodes in network. As the nodes in MANET are free to move, so MANET has dynamic, autonomous topology. MANET is very applicable in an environment where wired network is not available but communication is necessary like Battlefield communication, disaster area etc. In MANET a routing protocol is needed to find a path so as to transmit data packets between source and destination. The aims of routing protocols are discussed in this paper. Performance of MANET depends on the routing protocol scheme employed. Hence for efficient communication designing of a routing protocol is very challenging in dynamic topology. A number of protocols are discussed in this paper like Optimized Link State Routing (OLSR), Ad-hoc on Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Destination Sequence Distance Vector (DSDV) Such types of protocols are evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, ability to scale, etc.
The vision of Ad-Hoc networks is wireless internet, where users can move any where any time and still remaining connected with the rest of the world. [1]
Ad-Hoc is a Latin word and means “for this purpose”. [2]

II. AD-HOC ROUTING PROTOCOLS
Ad-Hoc routing protocols [3] are generally three types, Reactive (On-Demand), Proactive (Table-Driven) and Hybrid. Reactive protocols only search for a path between nodes when there is data to send. Reactive routing protocols have their own advantages of not wasting network Bandwidth with control message when data

transmission is not required. On the other hand Proactive protocols continuously establish and maintain routing paths for nodes whether data needs to be transferred or not. This comes at the cost of higher network management overhead in both network control messages and computational processing. Hybrid routing protocols exhibit both reactive and proactive properties. Hybrid protocols are more complex in nature. Establishment of such type of protocol has more complexity. Various protocols are described below.

A. OLSR

Optimized link state routing protocol (OLSR) [4] is based on link state algorithm and it is proactive in nature. OLSR is an optimization over a pure link state protocol [5] as it squeezes the size of information send in the messages, and reduces the number of retransmissions. It provides optimal routes in terms on number of hops. In this protocol topology information is periodically exchanged by using of link state messages. It reduces control overhead and connection. Unlike DSDV and AODV, OLSR reduces the size of control packet by declaring only a subset of links with its neighbors. In OLSR, each node uses the most recent information to route a packet. Hop by hop routing is used in forwarding packets. The use of Multipoint relay selectors (MPR) in OLSR is the distinctive feature over other classical link state protocols. In OLSR, only node selected as MPRs forward control traffic, reducing the size of control message.

B. AODV

Ad-Hoc On-Demand routing protocol (AODV) is a reactive protocol. This protocol can reduce the number of broadcasts by creating routes on demand. To find a path to the destination, a route request packet (RREQ) is broadcasted by the source till it reaches an intermediate node that has recent route information about the destination. AODV uses only symmetric links because the RREQ packet follows the reverse path of the RREQ. Unlike DSDV [6], AODV provides loop free routes in case of link breakage. The RREQ packet contains a sequence number and a broadcast id. Unlike DSDV, in AODV, if node cannot satisfy RREQ, it keeps track of the necessary information in order to implement the reverse and forward path setup that will accompany the transmission of the route reply (RREP). The source node can begin data transmission as soon as the first RREO is received.

C. DSR

The Dynamic Source Routing (DSR) protocol requires each transmitted packet to carry the full address from the source to the destination likewise the mechanism used in AODV. This mechanism in DSR makes it not to perform effectively in large networks, since the amount of overhead carried in these packets is increased as the size of the networks grows. Hence in highly dynamic and large networks, the overhead may consume a large amount of bandwidth. However this protocol has a number of advantages over routing protocols such as AODV and TORA (Temporally Ordered Routing Algorithm) [7] and in moderately small size network, this protocol performs better.

D. DSDV

The protocol Distance-Sequence Distance Vector (DSDV) [8] is a proactive (table-driven) routing protocol. This protocol solves the major problem associated with the distance vector routing of wired networks, by using destination sequence number. It maintains [9] a routing table that list all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The routing table update can be sent in two ways: a “full dump” or an incremental update.

III. COMPARISION OF PROACTIVE AND REACTIVE PROTOCOLS IN MANET

In this paper a classification of several routing schemes according to their routing strategy, table-driven and on demand is provided. A comparison of these two categories of routing protocols is presented, highlighting their

features, differences, and characteristics in TABLE I. The table-driven routing protocols maintain network connectivity proactively whereas On-demand routing protocols do the routing when it is needed. In proactive routing flat addressing can be simple to implement, however this method may not scale good for large networks [10]. Hence a comparison table is given here:

Routing Class	**Proactive (Table-Driven)**	**Reactive (On-Demand)**
Routing structure	Both Flat and hierarchical structures	Mostly Flat, Except CBRP
Availability of route	Always available	Determined when needed
Control Traffic volume	Usually high	Lower than proactive routing protocols
Periodic updates	Yes, some may use conditional.	Not required. Some nodes may require periodic beacons.
Control Overhead	High	Low
Route acquisition delay	Low	High
Storage Requirements	High	Depends on the number of routes kept or required. Usually lower than proactive protocols
Bandwidth requirement	High	Low
Power requirement	High	Low
Delay level	Small since routes are predetermined	Higher than proactive
Scalability problem	Usually up to 100 nodes.	Source routing protocols up to few hundred nodes. Point-to-point may scale higher
Handling effects of mobility	Occur at fixed intervals. DREAM alters periodic updates based on mobility	Usually updates ABR introduced LBQ AODV uses local route discovery
Quality of service support	Mainly shortest path as the QoS metric	Few can support QoS , Although most support shortest path

TABLE I COMPARISION OF PROACTIVE AND REACTIVE PROTOCOLS

IV. QUALITY OF SERVICE (QoS)

QoS[11] is a set of service requirements to be met by the network while transporting a flow. A flow is a packet stream from a source to a destination (unicast or multicast) with an associated (QoS). The associated QoS could, in fact, be 'best effort'. A fundamental requirement of any

QoS mechanism is a measurable performance metric. Typical QoS metrics include available bandwidth, packet loss rate, estimated delay, packet jitter, hop count and path reliability.

Due to the broadcast and dynamic nature of Mobile As-Hoc networking (MANET), providing QoS other than best effort, is a very challenging task. But QoS is important for the MANET to interconnect with wired networks which support QoS (e.g. A.T.M, Internet, etc.) and for real time applications. In the field of computer networking, QoS is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications, since these often requires fixed bit rate and are delay sensitive and in network where the capacity is a limited resource. Analogous to today's Internet, ad hoc networks are being designed to provide best-effort service (i.e. do not provide any guarantees regarding packet loss or delay, available bandwidth, jitter etc.). In a best-effort service model, packets are dropped regardless of their importance. If a packet is lost, the sender can simply retransmit the lost packet. This method is efficient for applications that do not require bounds on packet delay or other QoS metrics. However, real-time applications, such as video-on-demand (VoD), videoconferencing and Internet telephony have, are sensitive to packet loss and delay and may have minimum bandwidth requirements Consequently, the best-effort service may not be suitable for these applications.

A. Layered Architecture of QoS

The layered view/architecture [12] of quality of service contains 3 parts

- User
- Application
- Network

I) Application Layer QoS:

This layer explain how well user expectations are qualitatively satisfied such as clear voice (mean opinion scoring), jitter –free video, etc. This layer also describes arrival pattern and sensitivity to delivery delays. End-to- end protocols (RTP/RTCP), application-specific representations and encoding (FEC, interleaving) are implemented at this layer.

II) Network Layer QoS:

This layer four quality factors:

- Bandwidth - the rate at which an application's traffic must be carried by the network.
- Latency - the delay that an application can tolerate in delivering a packet of data.
- Jitter - the variation in latency.
- Loss - the percentage of lost data.

V. QoS MODEL

Generally, a QoS model does not define specific protocols or implementations. Instead the QoS model specifies the architecture in which some kinds of services could be provided in the network. It is the system goal to be achieved. The Flexible QoS Model for MANET (FQMM) [13] is based both on IntServ and DiffServ. Specifically, for applications with high priority, per flow QoS guarantees of IntServ are provided. On the other hand, applications with lower priorities achieve Diffserv per class differentiation. FQMM are applicable for both IntServ and DiffServ for different priorities, the drawbacks related to both still remain there.

VI. QoS ROUTING IN MANET

QoS routing is an essential part of the QoS architecture.

Before any connections can be made or any resources reserved, a feasible path between a source-destination pair must be established. QoS routing is a routing mechanism under which paths for flows are determined on the basis of some knowledge of resource availability in the network as well as the QoS requirements of the flows or connections [14]. The QoS routing supports QoS-Driven selection and QoS Reporting and provides path information at each router. The goal for QoS routing two factors:

- The QoS routing schemes can help admission control. That is, routing protocol not provides route to destination, but also computes the QoS, that is supportable on a route during the process of route computation. It accepts a new connection request, if it finds a suitable loop-free path from the source to destination having necessary resources (bandwidth) available to meet the QoS requirements of desired services, otherwise the connection request is rejected.

- QoS routing scheme that considers multiple constraints provide better load balance by allocating traffic on different paths subject to the QoS requirements of different traffics.

Ticket-based Probing Algorithm [15] is an example of QoS routing protocol. The basic idea in using tickets is to limit the number of candidate paths searched. QoS routing protocols include Preemptive Routing, Multipath Routing and Power Aware Routing.

VII. SECURITY ISSUES ON MANET

Performing communication in free space and the broadcast nature of Ad-Hoc networks expose it to security attacks. The mobile ad hoc network has the following typical features [16]:

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviours than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks. Understanding possible form of attack is always the first step towards developing good security solutions.

Mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defence in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network [17]. Another threat is compromised nodes inside the node. A good example of this kind of threats comes from the potential Byzantine failures encountered in the routing protocol for the mobile ad hoc network [18]. We call it a Byzantine failure when a set of nodes are compromised in such a way that the incorrect and malicious behaviour cannot be

directly detected because of the cooperation among these compromised nodes when they perform malicious behaviours. Byzantine failure is very harmful to the mobile ad hoc network. As we all know, due to the mobility of nodes in the ad hoc network, it is common that the nodes in the ad hoc network will reply on battery as their power supply method. While nodes in the wired network do not need to consider the power supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems. The first problem that may be caused by the restricted power supply is denial-of-service attacks [16].

VIII. SECURITY SOLUTIONS TO THE MANET

For the efficient use of MANET we need to establish a secure network to prevent data loss or malicious attack. Intrusion detection is not a new concept in the network research. According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [18]. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. The Intrusion-Resistant Ad-Hoc routing Algorithm (TIARA) [19] is designed against Denial of Service attacks. The TIARA mechanisms limit the damage caused by the intrusion attacks and allow for continued network operations at an acceptable level during such attacks. The Authenticated Routing for Ad-hoc network (ARAN) protocols is an on-demand, secure, routing protocol that detects and protects against malicious action carried out by the third parties in the ad-hoc environment. The Secure Efficient Ad-hoc Distance (SEAD) is a proactive secure routing protocol based on DSDV. SEAD deals with attackers that modify a routing table update message.

IX. CONCLUSION

This paper presents information about MANET, number of routing protocols for MANET, QoS and various security issues. Protocols used in MANET, which are broadly categorized as proactive and reactive. Proactive routing protocols tend to provide lower latency than that of the on-demand protocols, because they try to maintain routes to all the nodes in the network all the time. But the drawback for such protocols is the excessive routing overhead transmitted, which is periodic in nature without much consideration for the network mobility or load. On the other hand, though reactive protocols discover routes only when they are needed, they may still generate a huge amount of traffic when the network changes frequently. Depending on the amount of network traffic and number of flows, the routing protocols could be chosen. When there is congestion in the network due to heavy traffic, in general case, a reactive protocol is preferable. We have discussed about QoS for MANET, which is a set of services which must be met to the network during transmission. MANET has dynamic topology, so fulfilment of the required services is a challenging task. MANET is a dynamic free space communication network, so there are few issues because of which third party devices harm this topology frequently. Existing protocol has several issues which are still open, to minimizes the issue various research work is going on by considering a variety of practical parameter. To protect MANET from data loss, unwanted gathering security issues should be taken carefully.

REFERENCES

1. Giordano, S, 2002. Mobile ad-hoc networks. In: I. Stojmenovic (Ed.), Handbook of wireless Networks and Mobile Computing. Wiley, New York, pp: 325-343, 371-391
2. Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. Retrived 2009-01-02
3. M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," Ad Hoc Networks, vol. 2, no. 1, pp. 1–22, January 2004.
4. S. R. Das, R. Castaneda and J. Yan, "Simulation Based Performance Evaluation of Mobile Ad Hoc Network Routing Protocols," In Proceedings of Seventh International Conference on Computer Communications and Networks (ICCCN'98), 1998.
5. A. Boukerche, "Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks," Mobile Networks and Applications, pp. 9, 333-342, Kluwer Academic Publishers, 2004.
6. Farhat Anwar, Md. Saiful Azad, Md. Arafatur Rahman, and Mohammad Moshee Uddin (2008), Performance Analysis of Ad hoc Routing Protocols in Mobile WiMAX Environment, IAENG International Journal of Computer Science, Volume 35, Issue 3, September 2008, ISSN 1819-656X, pp 353-360.
7. V. D. Park and M. S. Corson." A highly adaptive distributed routing algorithm for mobile wireless networks". In INFOCOM'97, volume 3, pages 1405–1413, Kobe, Japan, April 1997.
8. Charles E. Perkins and Pravin Bhagwat,"Highly dynamic Destination Sequenced Distance Vector routing (DSDV) for mobile computers", Proc. SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, pages 234-244, August 1994.
9. V. Ramesh, Dr. P. Subbaiah, N. Koteswar Rao and M. Janardhana Raju,"Performance comparison and analysis of DSDV and AODV for MANET," (JJCSE) International Journal on Computer Science and Engineering , vol. 02 , pp. 183-188, 20 I 0
10. M. Jiang, J. Ji, Y.C. Tay, Cluster based routing protocol, Internet Draftbrp protocol, work in progress, 1999.
11. Crawley E, Nair R, Rajagopalan B, Sandrick H. A Framework for QoS Based Routing in the Internet. RFC 2386, August 1998.
12. Seema Department of Computer Science Engineering U.I.E.T (MDU), Rohtak, Haryana, India Dr. Yudhvir Singh Department of Computer Science Engineering U.I.E.T (MDU), Rohtak, Haryana, India Mr. Vikas Siwach Department of Computer Science EngineeringU.I.E.T (MDU), Rohtak, Haryana, India. Quality of service in MANET, 2012.
13. Xiao. H., W. K. G. Seah, A. Lo and K. C. Chua, 2000. A flexible quality of service model for mobile ad-hoc networks, IEEE VTC2000-spring, Tokyo, Japan, May, 2000
14. Crawley E, Nair R, Rajagopalan B, Sandrick H. A Framework for QoS Based Routing in the Internet. RFC 2386, August 1998.
15. Chen, S. And K. Nahrstedt, 1999. Distributed Quality-of-service routing in Ad hoc Networks. IEEE J. Selected Areas in Communication, 17: 1488-1505
16. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
17. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.
18. Intrusion-detection system, from Wikipedia, the free encyclopedia,http://en.wikipedia.org/wiki/Intrusion-detection_system.
19. Forman, G. H. And J. Zahorjan, 1994. The challenges of mobile computing. IEEE computer, pp: 38-47