ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A Study on Issues and Challenges in Mobile Ad hoc Networks

V.Jayalakshmi[1], Dr. T. Abdul Razak[2]

Research Scholar, Research and Development Center, Bharathiar University, Coimbatore, India[1]

Associate Professor, Dept. of Computer Science, Jamal Mohamed College, Tiruchirappalli, India[2]

ABSTRACT: Ad hoc networks are characterized by multihop wireless connectivity, frequently changing network topology and the need for efficient dynamic routing protocols. Traditionally, tactical networks have been the only communication networking application that followed the ad hoc paradigm. Recently, the introduction of new technologies such as the Bluetooth, IEEE 802.11 and Hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent evolutions have been generating a renewed and growing interest in the research and development of MANET. This paper attempts to provide a comprehensive overview of this dynamic field. It first explains the various routing protocols and then we present several challenges and issues in the Adhoc networking.

KEYWORDS: Routing Protocols, MANET, Security, QoS

I. INTRODUCTION

.

A mobile ad hoc network is a mobile, multihopwireless network that does not rely on any pre-existing infrastructure. Mobile ad hoc networksare characterized by dynamic topologies due touncontrolled node mobility, limited and variable sharedwireless channel bandwidth, and wireless devicesconstrained by battery power. One of the key challengesin such networks is to design dynamic routing protocolsthat are efficient, that is, consume less overhead.A new class of on-demand routing protocols(e.g., DSR [1,2], TORA [3], AODV [4,5]) formobile ad hoc networks has been developed withthe goal of minimizing the routing overhead. Theseprotocols reactively discover and maintain only theneeded routes, in contrast to proactive protocols (e.g.,DSDV[6]) which maintain all routes regardless of theirusage. The key characteristic of an on-demand protocolis the source-initiated route discovery procedure.Whenever a traffic source needs a route, it initiates aroute discovery process by sending a route request forthe destination (typically via a network-wide flood) andwaits for a route reply. Each route discovery flood isassociated with significant latency and overhead. Thisis particularly true for large networks. Therefore, foron-demand routing to be effective, it is desirable tokeep the route discovery frequency low.

The main challenge of MANETs is to route with low overheads even when conditions are dynamic. Overhead here is defined in terms of routing protocol control messages which consume both channel bandwidth as well as the battery power of nodes for communication/processing. Existing routing protocols in ad-hoc networks utilize the single route that is built for source and destination node pair. Due to node mobility, node failures and the dynamic characteristics of the radio channel, links in a route may become temporarily unavailable, making the route invalid. The overhead of finding alternative routes mounts along with additional packet delivery delay.

This paper is organized as follows. Section II provides details of the various classifications of protocols. Section III gives the issues of MANET. Section IV discusses the challenges in the Adhoc networks and we conclude the paper in Section V.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

II. Routing Protocols in Ad hoc Networks

The basic routing problem is that of finding an ordered series of intermediate nodes that can transport a packet across a network from its source to its destination by forwarding the packet along this series of intermediate nodes. In traditional hop-by-hop solutions to the routing problem, each node in the network maintains a routing table: for each known destination, the routing table lists the next node to which a packet for that destination should be sent.

The routing table at each node can be thought of as a view into part of a distributed data structure that, when taken together, describes the topology of the network. The goal of the routing protocol is to ensure that the overall data structure contains a consistent and correct view of the actual network topology. If the routing tables at some nodes were to become inconsistent, then packets can loop in the network. If the routing tables were to contain incorrect information, then packets can be dropped. The problem of maintaining a consistent and correct view becomes harder as there is an increase in the number of nodes whose information must be consistent, and as the rate of change in the actual topology increases.

The challenge in creating a routing protocol for ad hoc networks is to design a single protocol that can adapt to the wide variety of conditions that can be present in any ad hoc network over time. For example, the bandwidth available between two nodes in the network may vary from more than 10 Mbps to 10 Kbps or less. The highest speeds are achieved when using high-speed network interfaces with little interference, and the extremely low speeds may arise when using low-speed network interfaces or when there is significant interference from outside sources or other nodes' transmitters. Similar to the potential variability in bandwidth, nodes in an ad hoc network may alternate between periods during which they are stationary with respect to each other and periods during which they change topology rapidly. Conditions across a single network may also vary, so while some nodes are slow moving, others change location rapidly.

The routing protocol must perform efficiently in environments in which nodes are stationary and bandwidth is not a limiting factor. Yet, the same protocol must still function efficiently when the bandwidth available between nodes is low and the level of mobility and topology change is high. Because it is often impossible to know a priori what environment the protocol will find itself in, and because the environment can change unpredictably, the routing protocol must be able to adapt automatically

A. *Categories of Existing Routing Protocols for MANETs*

Many protocols have been proposed for MANETs. These protocols can be divided into three categories: proactive, reactive, and hybrid. Proactive methods maintain routes to all nodes, including nodes to which no packets are sent. Such methods react to topology changes, even if no traffic is affected by the changes. They are also called table-driven methods. Reactive methods are based on demand for data transmission. Routes between hosts are determined only when they are explicitly needed to forward packets. Reactive methods are also called on-demand methods. They can significantly reduce routing overhead when the traffic is lightweight and the topology changes less dramatically, since they do not need to update route information periodically and do not need to find and maintain routes on which there is no traffic. Hybrid methods combine proactive and reactive methods to find efficient routes, without much control overhead.

Proactive Routing Protocols

Proactive routing protocols described in [3, 6] attempt to maintain consistent and up-to-date routing information (routes) from each node to every other node in the network. Topology updates are propagated throughout the network in order to maintain a consistent view of the network. Keeping routes for all destinations has the advantage that communication with arbitrary destinations experiences minimal initial delay. Furthermore, a route could be immediately selected from the route table. However, these protocols have the disadvantage of generating additional control traffic that is needed to continually update stale route entries. Especially in highly mobile environments, communication overhead incurred to implement a proactive algorithm can be prohibitively costly. Typical and well-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

known examples of proactive routing protocols are destination-sequence distance vector (DSDV) [6] and optimized link state routing (OLSR) [10].

Reactive routing protocols

Reactive routing protocols proposed in [2,4,5] establish routes only when they are needed. When a source node requires a route to a destination, it initiates a route discovery process by flooding the entire network with a route request (RREQ) packet. Once a route has been established by receiving a route reply (RREP) packet at the source node, some form of route maintenance procedure is used to maintain it, until either the destination becomes inaccessible or the route is no longer desired. These protocols use less bandwidth for maintaining the routing tables at every node compared to proactive routing protocols by avoiding unnecessary periodic updates of routing information. However, route discovery latency can be greatly increased, leading to long packet delays before a communication can start. Ad hoc on-demand distance vector (AODV) [4] and dynamic source routing (DSR) [2] are well-known examples of reactive routing protocols.

Hybrid routing

A hybrid routing protocol [7-9] attempts to combine the best features of proactive and reactive algorithms. It often consists of the two classical routing protocols: proactive and reactive. Hybrid protocols divide the network into areas called zones which could be overlapping or non-overlapping depending on the zone creation and management algorithm employed by a particular hybrid protocol. The proactive routing protocol operates inside the zones, and is responsible for establishing and maintaining routes to the destinations located within the zones. On the other hand, the reactive protocol is responsible for establishing and maintaining routes to destinations that are located outside the zones. The zone-based routing protocol (ZRP) [7] and sharp hybrid adaptive routing protocol (SHARP) [9] are well-known examples of hybrid routing protocols..

Proactive vs. Reactive vs. Hybrid Routing

The tradeoffs between proactive and reactive routing strategies are quite complex. Which approach is better depends on many factors, such as the size of the network, the mobility, the data traffic and so on. Proactive routing protocols try to maintain routes to all possible destinations, regardless of whether or not they are needed. Routing information is constantly propagated and maintained. In contrast, reactive routing protocols initiate route discovery on the demand of data traffic. Routes are needed only to those desired destinations. This routing approach can dramatically reduce routing overhead when a network is relatively static and the active traffic is light. However, the source node has to wait until a route to the destination can be discovered, increasing the response time. The hybrid routing approach can adjust its routing strategies according to a network's characteristics and thus provides an attractive method for routing in MANETs. However, a network's characteristics, such as the mobility pattern and the traffic pattern, can be expected to be dynamic. The related information is very difficult to obtain and maintain. This complexity makes dynamically adjusting routing strategies hard to implement.

B. ***Basic Routing Protocol families***

Distance vector routing protocols

In distance vector routing protocols, every host maintains a routing table containing the distance from itself to possible destinations. Each routing table entry contains the next hop to the destination and the distance to the destination. Nodes only feed the estimated link costs for each destination (e.g. the number of hops to destination) to their neighbours, instead of flooding the whole network. All nodes calculate the shortest paths to the destinations using that broadcasted information.

Link state routing protocols

Link state routing protocols [10] keep a routing table for complete topology, which is built up by finding shortest path of link costs. Link cost information is periodically transmitted and received by all nodes using a flooding

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

technique, these periodic floods are called Link State Advertisements (LSA). Flooding means that a node sends out his information to all other neighbour nodes and they forward all received information to their neighbours and so on. Each node updates its table using the new link cost information gathered from these floods.

Source routing protocols

In source routing, all data packets carry their routing information as their header. The originating node could learn this routing information e.g. by means of a source routing protocol: When a node receives a (broadcast) route request packet for a destination it adds its own address to the header and then forwards the packet. The destination uses the recorded route in reverse order to send a route reply to the requesting node. Thus, the originating node is provided with the complete route to the destination. The routing decision is made at departure. Loops are avoided, since nodes can determine if they are already in the packet header.

III. ISSUES IN MANETS

If there are only two nodes to communicate with each other and are located very closely to each other, then no specific routing protocols or routing decisions are necessary. On the other hand, if there are a number of mobile hosts wishing to communicate, then the routing protocols come into picture, in this case some critical decisions have to be made such as which is the optimal route from the source to the destination which is very important because, the mobile nodes operate on battery power. Thus it becomes necessary to transfer the data with the minimal delay to loss less power. There will be kind of compression involved in which it could be provided by the protocol to loss less bandwidth. Further, there is need of encryption to protect the data from prying eyes. In addition to this, Quality of Service support is also needed so that the least packet drop can be obtained. The other factors which need to be considered while choosing a protocol for MANETs are as follows:

i. *Multicasting*: The ability to send packets to multiple nodes at once. This is similar to broadcasting except the fact that the broadcasting is done to all the nodes in the network. This is important as it takes less time to transfer data to multiple nodes.

ii. *Loop Free*: A path taken by a packet never transits the same intermediate node twice before it arrives at the destination. To improve the overall performance in the routing protocol to guarantee that the routes supplied are loop-free. This avoids any loss of bandwidth or CPU consumption.

iii. *Multiple routes*: If one route gets broken due to some disaster, then the data could be sent through some other route. Thus the protocol should allow creating multiple routes.

iv. *Distributed Operation*: The protocol should be distributed. It should not be dependent on a centralized node.

v. *Physical security*: Mobile networks are more vulnerable to physical security threats such as eavesdropping and jamming attacks.

vi. *On demand operation*: Since a uniform traffic distribution cannot be assumed within thenetwork, the routing algorithm must adapt to the traffic pattern on a demand or need basis,thereby utilizing power and bandwidth resources more efficiently..

vii. *Unidirectional Link Support*: The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

viii. *Entering/Departing nodes*: A routing protocol should be able to quickly adapt to entering ordeparting nodes in the network, without having to restructure the entire network.

IV. CHALLENGES IN MANETS

As shown in the figure 1, the research activitieswill be grouped, according to a layered approachinto three main areas:

- Enabling technologies;

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

• Networking;
• Middleware and applications

A. ***Security Attacks***

Securing wireless ad hoc networks is a highlychallenging issue. Understanding possible form ofattacks is always the first step towards developinggood security solutions. Ad hoc networks have tocope with the same kinds of vulnerabilities as theirwired counterparts, as well as with new vulnerabilitiesspecific to the ad hoc context. Furthermore,traditional vulnerabilities are alsoaccentuated by the ad hoc paradigm. Below wesummarize only the main directions of security inad hoc networks.

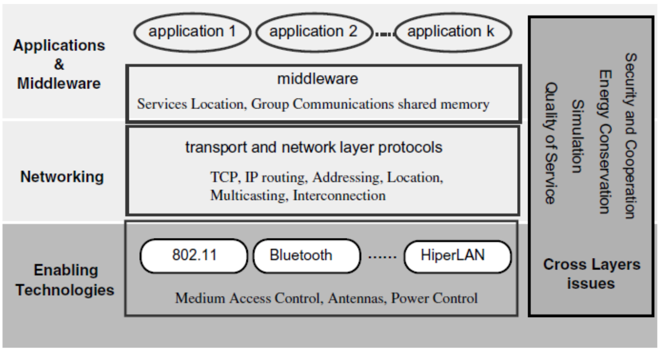

Fig. 1. A simple MANET architecture

Performing communication in free space exposesad hoc networks to attacks as anyone canjoin the network, and eavesdrop or inject messages.Ad hoc networks attacks can be classified as passive or active . Passive attack signifies thatthe attacker does not send any message, but justlistens to the channel. A passive attacks does notdisrupt the operation of a protocol, but only attemptsto discover valuable information. Duringan active attack, on the other hand, information isinserted into the network.

Passive eavesdropping is a passive attack thatattempts to discover nodes information (e.g., IPaddresses, location of nodes, etc.) by listening torouting traffic. In a wireless environment it isusually impossible to detect this attack, as it doesnot produce any new traffic in the network.

Active attacks involve actions such as the replication,modification and deletion of exchangeddata. Certain active attacks can be easily performedagainst an ad hoc network. These attackscan be grouped in : Impersonation, Denial of service, and Disclosure attack.

B. ***Mobility Models***

The ability of ad hoc networks_ protocols tocorrectly behave in a dynamic environment, wheredevices position may continuously change, is a keyissue. Therefore, modeling user'smovements is animportant aspect in ad hoc network simulation.
This includes among others :

- the definition of the simulated area in whichusers movements take place, and the rules formodeling users that moves beyond the simulatedarea;
- the number of nodes in the simulated area, andthe allocation of nodes at the simulation startup; and
- the mobility model, itself.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Typically, simulation studies assume a numberof users that moves inside a closed rectangulararea. Closed here stands for a constant number ofusers inside the simulated area. Rules are definedfor users arriving at the edges of the area.

The random waypoint mobility model is themodel most commonly used to define the wayusers move in the simulated area. According tothis model, nodes move according to a broken linepattern, standing at each vertex for a modeldefined pause time . arrives at its destination, it pauses for a time p,then chooses (draws) another destination and continues onward.

Recent studies have pointed out problems in therandom waypoint model. Two specific types ofproblems have been identified:

(i) the nodes average speed is decreasing, and
(ii) the nodes distributionin the simulated area is non-uniform.

C. *Quality of service*

Providing Quality of Service (QoS), other thanbest effort, is a very complex problem in MANETs,and makes this area a challenging area of future MANET research.. Network's ability to provide QoS depends on the intrinsic characteristicsof all the network components, fromtransmission links to the MAC and network layers. MANET characteristics generally lead to theconclusion that this type of network provides aweak support to QoS. Wireless links have a (relatively)low and highly variable capacity, and highloss rates. Topologies are highly dynamic withfrequent links breakages. Random access-basedMAC protocols, which are commonly used in thisenvironment (e.g., 802.11b), have no QoS support.Finally, MANET link layers typically run in unlicensedspectrum, making it more difficult toprovide strong QoS guarantees in spectrum hardto control. This scenario indicates that, notonly hard QoS guarantees will be difficult toachieve in a MANET, but if the nodes are highlymobile even statistical QoS guarantees may beimpossible to attain, due to the lack of sufficientlyaccurate knowledge (both instantaneous and predictive) of the network states. Furthermore,since the quality of the network (in terms ofavailable resources reside in the wireless mediumand in the mobile nodes: e.g., buffer and batterystate) varies with time, present QoS models forwired networks are insufficient in a self-organizingnetwork, and new MANET QoS model must be defined .

V. CONCLUSIONS

In coming years, mobile computing will keepflourishing, and an eventual seamless integrationof MANET with other wireless networks, and thefixed Internet infrastructure, appears inevitable. The opportunity and importanceof ad hoc networks is being increasingly recognizedby both the research and industry community.In moving forward towards fulfilling this opportunity, the successful addressing ofopen technical and economic issues will play a critical role inachieving the eventual success and potential of MANETtechnology. Much work remains to be done on cost-effective implementation issues to bring the promise of ad hoc networks within the reach of the public.

REFERENCES

[1] Johnson D, Maltz D. Dynamic source routing in ad hoc wireless networks. In Mobile Computing, chapter 5, Imielinski T, Korth H (eds). Kluwer Academic: Hingham, MA, USA, 1996.
[2] Johnson DB, Maltz DA, Hu Y. The dynamic source routing protocol for mobile ad hoc networks .
[3] Park VD, Corson MS. A highly adaptive distributed routing algorithm for mobile wireless networks. In *Proceedings of IEEE Infocom*, 1997.
[4] Perkins CE, Royer EM. Ad hoc on-demand distance vector routing. In Proceedings of IEEEWorkshop on Mobile Computing Systems and Applications (WMCSA), 1999.
[5] Perkins CE, Belding-Royer E, Das SR. Ad hoc on-demand distance vector (AODV) routing. http://www.ietf.org/rfc/rfc3561.txt, July 2003. RFC 3561.
[6] Perkins CE, Bhagwat P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In Proceedings of ACM Sigcomm, 1994.
[7] A. Boukerche, L. Bononi, Simulation and modeling ofwireless, mobile and ad hoc networks, in: S. BasagniM. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.
[8] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) forAd Hoc Networks," IETF Mobile Ad Hoc Networking Working Group INTERNETDRAFT., July 2002.
L. Wang and S. Olariu, "A Two-Zone Hybrid Routing Protocol for Mobile Ad HocNetworks," IEEE Transactions on Parallel and Distributed Systems, vol. 15, pp.1105-1116, December 2004.
[9] V. Ramasubramanian, "SHARP: A Hybrid Adaptive Routing Protocol for Mobile AdHoc Networks," Proceedings ACM Mobihoc, pp. 303-314, June 2003
[10] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," IETFMobile Ad Hoc Networking Working Group INTERNET DRAFT, RCF 3626, October2003, http://www.ietf.org/rfc/rfc3626.txt, retrieved on December 2007.