



Behavioral Study of Issues And Challenges In Mobile Adhoc Network

Anju Gill

CSE Department

U.I.E.T. Kurukshetra University, Kurukshetra

Haryana, India

anjugill86@gmail.com

Chander Diwaker

Assist. Prof. CSE Department

U.I.E.T. Kurukshetra University, Kurukshetra

Haryana, India

Chander_cd@rediffmail.com

Abstract - Mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links without central infrastructure. Each node operates not only as an end system, but also as a router to forward the packets. The nodes are free to move about and organize themselves into a network and changes position frequently so that network topology unpredictably changes dynamically. Hence MANETS are best suited for the applications in which there is not requirement for existing underlying infrastructure. In this paper, the author will provide an overview of routing protocol, traffic types, underlying issues and challenges related to security, mobility and resource limitation and also give possible solution for them.

Keywords - Bandwidth-constrained, security, Unicasting, Multicasting, Energy conservation.

I. INTRODUCTION

Mobile ad-hoc network are gaining popularity in today scenario due to instant networking to people who may not lie within transmitting range of one another. It is a group of wireless mobile computers (or nodes); in which nodes collaborate with each other by forwarding packets for communication. Such networks have no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. The participating nodes act as routers to route the packet to proper destination. These networks are fully distributed, self-configuring and can work at any place without the need of any underlying infrastructure. This property makes the ad-hoc networks extremely robust [1].

In Figure 1 there are nodes A and C should discover the route through node B in order to communicate. The circles indicate range of each node. Nodes A and C are not inside the direct transmission range of each other, since A's circle does not cover C [2].

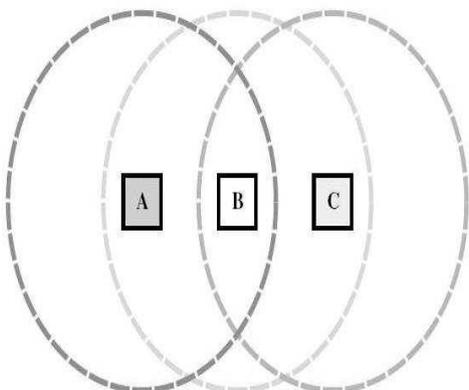


Fig. 1 Example of a simple ad-hoc network [2].

A. Characteristics

The ad hoc topology can modify with time as the nodes move in geographical area or adjust their transmission and reception parameters. Mobile Ad hoc Network has numerous salient characteristics that distinguish this from other kind of wireless networks [3]:

1) *Dynamic topologies*: Nodes in the network are free to move arbitrarily; i.e. network multi-hop topology may change randomly and rapidly unpredictably over time and may have of both unidirectional and bidirectional link.

2) *Bandwidth-Constrained variable capacity links*: Wireless links will continue to have considerably less capacity than their hardwired counter-parts. In addition, the output of wireless communications, after accounting for the effects of multiple access, noise, fading, and interference conditions, etc. is often much less than the radio's maximum transmission rate. One effect of relatively low to moderate link capacity is that congestion is usually the norm rather than the exception, i.e. aggregate application demand approaches or exceed network capacity frequently. As the mobile network is simply an extension of the fixed infrastructure network, mobile ad hoc users will demand same services. These demands will continuously increases as collaborative networking and multimedia computing applications rise.

3) *Heterogeneous network*: Ad-hoc network's nodes have dissimilar radio transmission and receiving (i.e. downstream and upstream) frequencies.

4) *Energy-constrained operation*: Nodes in a MANET may rely on battery life or other exhaustible means for their energy. For these nodes, a system design criterion for optimization and energy conservation is most important.

5) *Limited radio range*: Due to limited transmission power MANETs have limited radio range.

6) *Limited security*: MANET is generally more prone to physical security attacks and threats than the fixed-cable networks. The increased opportunity of spoofing, eavesdropping, and denial-of-service attacks must be carefully considered. Existing link security techniques can be applied within wireless networks to diminish security threats. As an advantage, the decentralized nature of MANETs provides additional robustness against the single points of failure.

7) *Mobile node functioning as a router*: Every mobile node runs a routing protocol. The participating nodes act as host as well as router.

B. Applications of MANET

Some of the applications of MANETs are as follows:

- **Military**: Homeland defense, automated battlefield, Special operations etc.
- **Civilian**: Search and rescue in remote areas, Disaster Recovery (flood, fire, earthquakes etc), Law enforcement (crowd control), Space/planet exploration, Environment monitoring (sensors).
- **Commercial**: Patient monitoring, Vehicle to Vehicle communications, Sport events, festivals, conventions, Ad hoc collaborative computing (Bluetooth), Sensors on cars (car navigation safety), Video games at amusement parks., etc [4].

II. MANET ARCHITECTURE

The nodes in a MANET can be classified by their capabilities. A Client or Small Mobile Host (SMH) is a node with reduced processing, storage, communication, and power resources. A Server or Large Mobile Host (LMH) is a node having a larger share of resources. Servers, due to their larger capacity contain the complete DBMS and bear the primary responsibility for data broadcast and satisfying client queries. Clients typically have sufficient resources to cache portions of the database as well as storing some DBMS query and processing modules.

In a MANET, each node has an area of control. This is the area over which its transmissions can be heard by other nodes and it can hear other transmission. A LMH will firstly have a larger area of influence as it usually has a more powerful battery. As the power level declines, the area of influence of any node will become smaller or shrink because the power available to broadcast is reduced. Network nodes may operate in any of three modes that are designed to facilitate the reduction in power used [5]:

- *Active Mode (or Transmit Mode)*: In this mode node uses the most of power. It allows both the transmission and reception of messages.
- *Doze Mode (or Receive Mode)*: In this mode the CPU is able to process information and is also capable of receiving acknowledgement of messages from other nodes and listening to broadcasts.
- *Sleep Mode (or Standby Mode)*: Here in this mode CPU does no processing and the node is not able to send/receive messages. The node remains inactive in this mode. In this mode a node turn itself off for short periods of time without requiring power-up or re-initialization.

A node that has no remaining power, or one that get turn off, is not currently a part of the network and is not be reachable by any other node. Nodes can become cut off from the entire network. When goes back in range of other nodes, they will happen to re-connected. Conversely, a node may be reachable by several LMHs or SMHs.

There are two approaches to providing network connectivity in a MANET:

A. Hierarchical network architecture:

In this approach the whole network is partitioned into sub-networks. Each of the sub-networks itself then dynamically select a node among themselves which acts as gateway to the other sub-network. This process builds a hierarchy among the nodes and this hierarchy can be one-tire hierarchy or multiple tier hierarchy. The advantages of this approach are:

- Better manageability.
- Easy mobility management procedures.

B. Flat-routed architecture:

In this approach in terms of responsibility all the nodes are identical, and there is no special gateways node is elected here all nodes have same features and responsibilities. The advantages of this approach are:

- Increased reliability / survivability due to no single point of failure
- Provides alternative routes in the network.
- Reduced use of wireless resources.
- Better load balancing property
- All nodes have one type of equipment.
- Optimal Routing

III. TRAFFIC TYPES IN MANET

The traffic in the network is basically the flow of packets in the network. The traffic types in ad hoc networks are quite different from an infrastructured wireless network's traffic types; adhoc networks include [5]:

A. Peer-to-Peer:

Peer-to-Peer Communication is between two nodes, which are at one hop distance. Network traffic is usually consistent.

B. Remote-to-Remote:

Remote-to-Remote communication is between two nodes away from a single hop but which preserve a stable route between them. This can be the result of a number of nodes staying within communication range of each other in a single area or maybe moving as a group. The traffic is similar to standard network traffic.

C. Dynamic Traffic:

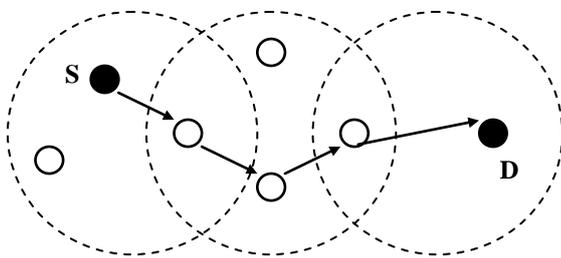
This type of traffic occurs in the case when nodes in the network are dynamic and moving around arbitrary. Routes must be reconstructed. This causes a poor connectivity and network activity in short bursts.

IV. ROUTING PROTOCOL

The basic operation in IP layer of MANET is to successfully transmit data packets from the source to the destination. Therefore, efficient routing of packets is a primary MANET challenge as it may be necessary to employ several hops i.e. multi-hop before a packet reaches the destination (see Figure. 2). The routing protocol has two main functions: (a)

selection of routes for various source-destination pairs, and (b) delivery of messages to their correct destinations. The forwarding procedure (delivery of message) of routing protocol simply uses a routing table in order to lookup for the destination address in the data packet. If the destination address is found in the routing table, the packet is sent to the corresponding next hop.

Unlike the nodes in a traditional hardwired network, the nodes in the MANET are free to move arbitrarily. As a result, the network topology changes more frequently than in the hardwired network. The routing in MANET is, therefore, intrinsically different from traditional routing found on fixed or infrastructured networks. On the bases of routing information update mechanism routing protocols of ad-hoc network can be classified into three categories. These are:



S- Source node, D- Destination node

Fig. 2 MANET routes packets in multiple hops

A. Proactive or table driven routing protocol

In table driven routing protocol nodes periodically exchange routing information in the form of routing table to maintain consistent and up-to-date view of the network when network topology changes. When node require a path to destination it runs appropriate path finding algorithm on topology information maintained by every node and floods routing information in the whole network. Routing table uses sequence number to find up-to-date route. Destination Sequence Distance Vector (DSDV), Global State Routing (GSR), and Clustered Gateway Switch Routing (CGSR) etc are some of the existing table-driven ad hoc routing protocols [6].

B. Reactive or on-demand routing protocol

These protocols do not maintain topology information and taken as a lazy approach to routing. In contrast to table-driven routing protocols routes are established as and when required i.e. no periodic exchange of routing information. The route remains valid until the route is no longer needed. Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector Routing (AODV) etc are routing protocol fall in this category [6].

C. Hybrid routing protocol

Hybrid routing protocol combines best features of above two protocol categories. Within a certain geographical domain a table driven approach is used and beyond this domain on-demand approach is applied. Zone Routing Protocol, (ZRP), Wireless Ad hoc Routing Protocol, (WARP) are routing protocol fall in this category.

V. CHALLENGES AND SOLUTION IN DESIGNING ROUTING PROTOCOLS FOR MANET

The conventional routing protocols in wired network such as Link State or Distance Vector are designed for static network topology [3]. However, ad hoc network is highly dynamic, which means that Link State or Distance Vector would have problems to converge to a steady state. Though, Link State or Distance Vector work well in ad hoc network with low mobility, the problem that still remains is that these are highly dependent on periodic control messages. Thus, the maintenance of routes in such protocols is costly in resources such as bandwidth, battery power and CPU.

High mobility nodes can impact the route maintenance overhead of routing protocols in such a way that no bandwidth might remain available for transmission of data packets. Thus, the low resource availability in these networks demand their efficient utilization and hence the motivation for optimal routing in ad hoc network [7, 8]

A critical look at the characteristics of MANET such as dynamic topology, energy constrained operations, bandwidth constrained links, limited security etc, indicate that the routing protocols need to address the following issues: -

A. Unicasting and Multicasting of packets:

Unlike typical Internet applications, most applications of MANET involve one-to-many and many-to-many communication patterns. The routing of messages in such networks become extremely challenging because of its inherent dynamic nature coupled with constraints like limited bandwidth, limited battery power, interference of signals, broadcast nature of wireless communication etc [9, 10]. Several ad hoc unicast and multicast routing protocols have been proposed, although ad hoc routing is still a relatively immature technology.

Solution:

MOMENTAP, a new multicast routing protocol for ad hoc environment has been designed that has drastically reduced the flooding of data packets by using smart algorithm called BNNSA. The number of control packets also been significantly decreased thereby reducing packet processing overhead as well as saving of costly battery back up.

B. Energy conservation

Mobile devices rely on battery for its power requirements. Since battery power is limited and represents one of the greatest constraints in designing algorithms for mobile devices. In fact, limitations on battery life and the additional energy requirement for supporting network operations (e.g. routing) inside each node, makes energy conservation one of the main concerns in MANET [11]. It is therefore vital that power utilization be managed efficiently by designing a routing protocol that use less power, preferably with no impact on applications.

Solution:

PESAR, a new power efficient routing protocol has been designed. In the proposed work, the lifetime of mobile nodes has been increased. At the same time, it has avoided eventuality of any network partitions by evenly distributing the power consumption rate to each node. Besides, the overall transmission power for each connection request has been minimized by drastically reducing the flooding of data packets.

C. Security

Security has become a critical issue between the mobile nodes in MANET because of the classical applications such as

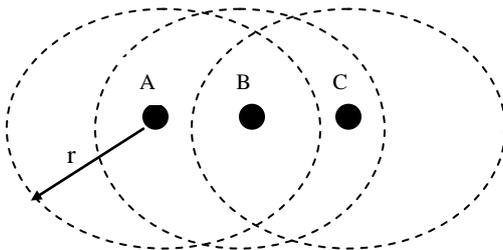
'tactical communication in a battlefield' (military application) where the environment is hostile and operation is security sensitive. However, unlike the wired network, the inherent characteristics of MANET such as wireless medium, highly dynamic topology, distributed cooperation, resource constrained capability, and limited physical security poses number of nontrivial security challenges to the network. Hence, enforcement of security through secure routing protocol becomes an extremely critical task.

Solution:

A multi-fenced security model has been proposed which embeds the various security components such as IP Security, Key Authentication, Intrusion Detection System, network security algorithms etc. in defence against both known and unknown threats.

D. Hidden terminal problem

Hidden terminal problem causes collision of packet at the receiving end due to simultaneous transmission of packet from the nodes that are not within the direct transmission range of each other but they are within the transmission range of receiver. E.g. as in figure 3 node A and C send packet to B at same time as a result there is collision at node B because A and C are hidden from each other i.e. not within direct transmission range of each other [6].



Here r is transmission range of node A

Fig. 3 Hidden Terminal Problem

Solution:

As a result of hidden terminal problem network performance and throughput is affected. MACA (Medium Access Collision Avoidance), MACAW (Medium Access Collision Avoidance for Wireless), FAMA (Floor Acquisition Multiple Access) and DBTMA (Dual Busy Tone Multiple Access) schemes defenses hidden terminal problem.

E. Exposed terminal problem

The Exposed Terminal Problem is inability of a node which is blocked for transmission when nearby node is transmitting to another node as in figure 4 if B transmission to A is in progress then node C can not send packet to D because B is neighbor of B which is transmitting now and hence must not interfere with on going transmission. Therefore reusability of radio spectrum is affected.

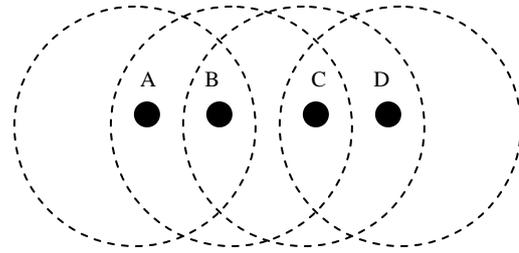


Fig. 4 Exposed Terminal Problem

Solution:

If node C and B both are transmitting then transmitting frequency of C will be different from the receiving frequency of node B.

F. Link unreliability

The appropriate functioning of the network not only depends upon the correct execution of the network but it requires adjustment according to dynamically exhibiting network topology. A link participation in packet forwarding process is dependent upon its movement and available resources which creates baneful effect in the network. The lost packets need to be transmitted again by optimal reconfiguration of the path.

Solution:

The problem caused due to link breakage can be controlled by priory appraising its reliability and associating trust level accordingly. Hence any node in the network must be issued with an off-line certificate by several other nodes depending on factors like mobility and limited resources.

G. Route Maintenance

Nodes in ad-hoc network are free to move arbitrary which causes dynamic change in topology and link breakage frequently. As an advantage of multi-hop nature of MANET, node search alternative path for packet forwarding to the destination. Dual transmission of data during alternate path establishment period will increase network traffic and time complexity.

Solution:

Conventional routing protocol involves route discovery and route maintenance via periodic routing update. Topology change or link breakage reflects change to all other node to change their routing information to compute new route to the destination. Preemptive routing scheme which discover alternative path before existing link breakage like soft handoff in mobile telephone networks can be adapted.

H. Network partitioning

Sometime ad-hoc network routing protocols not able to manage with network partitions; as a result a set of nodes behaves autonomously of others. This kind of partitioning causes degradation of network performance, and some rigorous consequences like non optimal routes and effect throughput etc.

Solution:

Network partition occurs due to node movement in or out of the networks and causes other nodes that were connected to the moving node get disconnected from the network. The connection can be reestablished through periodic beaconing.

I. Non-optimal routes

Non-optimal routes are results of malicious modification and inconsistent routing information exchange by attacker during packet forwarding. Due to highly dynamic nature of MANET link breaks and new path have to be searched which may not be optimal [12].

Solution:

Malicious or adversary node in the network create non-optimal path by forwarding inconsistent information in the network. This issue can be resolved by identifying and removing the adversary or by following second shortest path for traffic forwarding instead of first shortest path then the attacker will not be able to taint data transmission.

VI. CONCLUSION

In this paper, an effort has been made to concentrate on the overview, architecture and traffic types in mobile ad-hoc network. As MANET is appealing as “anywhere, anytime” network and due to dynamically changing topology, infrastructure less and decentralized nature of MANET, MANETs routing protocol faces various issues and challenges such as energy conservation, security, non-optimal route, hidden and exposed terminal problem etc and the solution to cop up these challenges have been discussed. These solutions cover a subset of vulnerabilities and are far from providing a comprehensive answer to the routing and security problems in MANETs. There are still some challenges that are still to be solved such as addressing, location management, asymmetric link etc in manets on which work is being going on to provide the better solution in future and better performance of routing protocol.

REFERENCES

- [1] G. Jayakumar and G. Ganapathy, “Performance Comparison of Mobile Ad-hoc Network Routing Protocol”, *International Journal of Computer Science and Network Security (IJCSNS)*, VOL.7 No.11, pp. 77-84, November 2007.
- [2] A. N. Thakare and M. Y. Joshi, “Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks” *IJCA* , pp 211-218, 2010.
- [3] I. Chlamtac, M. Conti, and J.-N. Liu, “Mobile ad hoc networking: imperatives and challenges,” *Elsevier Ad Hoc Networks Journal*, vol. 1, pp. 13–64, 2003.
- [4] M. Bheemalingaiah., “Energy Aware Node Disjoint Multipath Routing in Mobile Ad Hoc Network”, *Journal of Theoretical and Applied Information Technology, JAITIT*, pp. 416-417, 2005-2009.
- [5] Mobile Ad Hoc Networks (MANETs) Are Not A Fundamentally Flawed Architecture, URL: <http://www.cs.rutgers.edu/~rmartin/teaching/fall04/cs552/papers/012.pdf>.
- [6] C.Siva Ram Murthy and B.S Manoj, *Mobile Ad Hoc Networks- Architectures & Protocols* , Pearson Education, New Delhi, 2004.
- [7] A. Goel and A.K. Sharma, “A Comparative Study of Unicast Routing Protocols for Mobile Ad Hoc Network”, in *Proc. of National Conference on Communication, Information and Telemetric- An Indian Scenario (CITEL-2005)*, KCT, Coimbatore, Mar. 2005.
- [8] D. Leslie. Fife and Le Gruenwald, "Research issues for data communication in mobile ad-hoc network database systems", *ACM NY*, Volume 32, Issue 2, pages: 42-47 2003.
- [9] C.E. Perkins, *Ad Hoc Networking*, Addison-Wesley Longman, 2001.
- [10] C. C. Chiang, H. K. Wu, W. Liu, and M. Gerla, "Routing and Multicast in Multihop Mobile Wireless Networks", in *Proc. of IEEE Singapore International Conference on Networks (SICON'97)*, 1997.
- [11] C-K. Toh and V. Vassiliou, *The Effects of Beaconing on the Battery Life of Ad Hoc Mobile Computers*, Chapter 9, pp. 299.
- [12] B. R. Sujatha and M. V. Satyanarayana, “Improved Network Connectivity in MANETs”, *International Journal of Computer Networks & Communications (IJCNC)*, Vol.1, No.3, October 2009.