ANALYZING THE MANET VARIATIONS, CHALLENGES, CAPACITY AND PROTOCOL ISSUES

G. S. Mamatha[1] and Dr. S. C. Sharma[2]

[1]Department of Information Science and Engineering, R. V. College of Engineering, Bangalore, India
mamatha.niranjan@gmail.com
[2]Vice-Chancellor, Tumkur University, Tumkur, Karnataka, India
scsrvrd@yahoo.co.in

ABSTRACT

Various deployment ways of mobile ad hoc networks (MANETS) can have widely varying characteristics that have a greater impact on the behaviour of different routing protocols created for these networks. Before directly deploying the applications in such environments, it is most important for developers to understand the potential quantitative behaviour of the variations, challenges, capacity and implementation issues that support their applications. Analytical models exist to describe the behaviour of MANETS, but they are restricted to simplistic statistical models that represent either node mobility or link connectivity individually without considering the interplay of the two and other important aspects of MANETS. In this paper we are trying to analyze and study the MANET environments, challenges and other issues, which will help the researchers to understand the MANET concepts thoroughly.

KEYWORDS

MANETS, Variations, Challenges, Protocol, and Capacity.

1. INTRODUCTION

Mobile ad hoc networks (MANETS) due to its inherent capabilities of instant communication in most of the time and mission critical applications recently received a significant researchers attention.The main goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes which may be combined routers and hosts--they form the network routing infrastructure in an ad hoc fashion [1]. Lot of security vulnerabilities in a wireless environment, such as MANET, has been identified and a set of countermeasures were also proposed [2]. However, only a few of them provide a guaranty which is an orthogonal to security critical challenge [3]. Taking these factors into concern, the main vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links [1]. Considering this nature of MANETS, its environment consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internetwork. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be unidirectional (broadcast),

DOI : 10.5121/ijcses.2010.1102

highly-directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters [1]. In this paper we are describing the MANETS environment variations, challenges, capacity and some of the implementation and protocol issues taking in to consideration of the above mentioned characteristics of MANETS.

The paper is organized as: Section II gives description of MANET environment variations, Section III describes the MANET challenges, Section IV gives an insight to MANET capacities, Section V illustrates the protocol performance issues and finally with Concluding remarks.

2. MANET ENVIRONMENT VARIATIONS

The different MANET environment variations [4] are listed as follows taking its dynamic topology in to consideration:

1. In MANETS all nodes have identical capabilities and responsibilities, which are termed as fully symmetric environment. A mobile ad hoc network (MANET) is a network comprising wireless mobile nodes that communicate with each other without centralized control or established infrastructure. These nodes which are within each other's radio range can communicate directly, while distance nodes rely on their neighbouring nodes to forward packets. In MANETS every node can be a host or router. In MANET environment, nodes are free to join or leave the network at any point of time, resulting in a highly dynamic network environment compared to wired network [5].

2. The Asymmetric Capabilities in MANETS include transmission ranges and radios ranges which may differ. Battery life, speed of movement and processing capacity will be different at different nodes.

3. Asymmetric Responsibilities include that only some nodes may route packets in the network or some nodes may act as leaders for nearby nodes like cluster head.

4. Traffic characteristics may differ in different ad hoc networks like bit rate, timeliness constraints, reliability requirements, unicast or multicast or geocast, host-based addressing or content-based addressing or capability-based addressing.

5. MANETS may co-exist and also co-operate with an infrastructure based network.

6. Mobility patterns may be different like people sitting at an airport lounge, citywide taxi cabs, military movements and personal area networks. The performance of a mobile ad hoc network is dependent on the node mobility pattern as well as topology, data traffic patterns, and radio interference.

7. Mobility characteristics include speed, predictability, direction of movement, pattern of movement, uniformity of mobility characteristics among different nodes.

3. MANET CHALLENGES

The following list of challenges shows the inefficiencies and limitations that have to be overcome in a MANET environment [4]:

- Limited wireless transmission range: In wireless networks the radio band will be limited and hence data rates it can offer are much lesser than what a wired network can offer. This requires the routing protocols in wireless networks to use the bandwidth always in an optimal manner by keeping the overhead as low as possible. The limited

transmission range also imposes a constraint on routing protocols in maintaining the topological information. Especially in MANETS due to frequent changes in topology, maintaining the topological information at all nodes involves more control overhead which, in turn, results in more bandwidth wastage [6].

- Time-varying wireless link characteristics: The wireless channel is susceptible to a variety of transmission impediments such as path loss, fading, interference and blockage. These factors resist the range, data rate, and the reliability of the wireless transmission. The extent to which these factors affect the transmission depends upon the environmental conditions and the mobility of the transmitter and receiver. Even the two different key constraints, Nyquist's and Shannon's theorems, that govern the ability to transmit information at different data rates can be considered [6].
- Broadcast nature of the wireless medium: The broadcast nature of the radio channel, that is, transmissions made by a node are received by all nodes within its direct transmission range. When a node is receiving data, no other node in its neighbourhood, apart from the sender, should transmit. A node should get access to the shared medium only when its transmissions do not affect any on going session. Since multiple nodes may contend for the channel simultaneously, the possibility of packet collisions is quite high in wireless networks [6]. Even the network is susceptible to hidden terminal problem and broadcast storms [4]. The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver [6].
- Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as high bit error rate (BER) in the wireless channel, increased collisions due to the presence of hidden terminals, presence of interference, location dependent contention, uni-directional links, frequent path breaks due to mobility of nodes, and the inherent fading properties of the wireless channel [6].
- Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes. Therefore mobility management itself is very vast research topic in ad hoc networks.
- Mobility-induced packet losses: Communication links in an ad hoc network are unstable such that running conventional protocols for MANETS over a high loss rate will suffer from severe performance degradation. However, with high error rate, it is very much difficult to deliver a packet to its destination.
- Battery constraints: This is one of the limited resources that form a major constraint for the nodes in an ad hoc network. Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device. By increasing the power and processing ability makes the nodes bulky and less portable. So only MANET nodes has to optimally use this resource.
- Potentially frequent network partitions: The randomly moving nodes in an ad hoc network can lead to network partitions. In major cases, the intermediate nodes are the one which are highly affected by this partitioning.
- Ease of snooping on wireless transmissions (security issues): The radio channel used for ad hoc networks is broadcast in nature and is shared by all the nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So an attacker can easily snoop the data being transmitted in the network. Here

the requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered through snooping [6].

4. MANET CAPACITY

The different cases in which the throughput of the channel varies is a MANET is listed as follows [4]:

- Consider a single channel shared by n nodes in a network, then the throughput per node will be ***(1/n)***, on average.
- Consider an IEEE 802.11a/g channel at 54 Mbps in a network with single user, the capacity will be around 25-30 Mbps due to MAC overhead.
- For unit disk with n nodes and no mobility considered, the throughput per node will be ***(O (1/sqrt (n)))*** [7].
- For a chain (linear) of ad hoc nodes in a network, the ideal capacity will be 1/4 of channel; simulation yields capacity of 1/7 of channel [8].
- Consider the case in which the packets are distributed to many intermediate nodes that relay packet to destination when destination comes nearby in a network. In such cases the throughput per node will be ***(O (1))*** [9].
- Consider with multi-user coding in a network, then the throughput per node will be ***(O (1))*** [10].

4.1. Capacity of Fixed Ad Hoc Networks

- Let us consider ***n*** nodes in area ***A*** transmitting at ***W*** bits/sec using a fixed range (distance between a random pair of nodes is ***O (sqrt (n))***, then the bit-distance product that can be transported by the network per second is, ***(W sqrt (A n))***, then the throughput per node is ***(W / sqrt (n))*** [7].

4.2. Capacity of Mobile Ad Hoc Networks

- Let us assume random motion in a network, wherein any two nodes become neighbours once in a while and each node assumed sender for one *session,* and destination for another *session* and relay packets through at most one other node. Packet go from source to destination directly, when source and destinations are neighbours, or from source to a relay and the relay to destination, when each pair becomes neighbour respectively. In such a case the throughput of each session is ***O(1)***, which is independent of ***n***. Delay in packet delivery can be large if ***O(1)*** throughput is to be achieved and delay incurred waiting for the destination to arrive close to a relay or the sender [11].

5. MANET ROUTING PROTOCOL PERFORMANCE ISSUES

In order to judge the merit of a routing protocol, there is a need of both qualitative and quantitative metrics with which we can measure its suitability and performance. These metrics are always considered to be independent of any given routing protocol [1].

The following list shows some of the desirable qualitative characteristics of MANET routing protocols [1]:

1) Distributed operation: An Adhoc wireless network is totally distributed in nature, since nodes has to gain easy access to the broadcast channel. The use of any centralized control or routing approach in such networks will consume large amount of bandwidth.

2) Loop-freedom: Avoids problems such as, a small fraction of packets spinning around in the network for arbitrary time periods. Ad hoc solutions such as TTL (Time to Live) values can bind the problem, but a more structured and well-formed approach is generally desirable as it usually leads to better overall performance.

3) Demand-based operation: The dynamic topologies will lead to the routing algorithm adapt to the traffic pattern on a demand or need basis, instead of assuming a uniform traffic distribution within the network (and maintaining routing between all nodes at all times). If this has been carried out intelligently, the network energy and bandwidth resources are utilized more efficiently, at the cost of increased route discovery delay.

4) Proactive operation: This is very important property for a demand-based operation. As such in certain contexts, an extra additional latency demand-based operation incurs may not be acceptable. In such cases, if the bandwidth and energy resources of the network permit, then a proactive operation is desirable.

5) Security: If the ad hoc network lacks some form of network-level or link-layer security, a MANET routing protocol will be more vulnerable to many forms of malicious attacks. It can be simple attack like snooping network traffic, transmissions replay, manipulation of the packet headers, and redirecting the routing messages, within an Adhoc wireless network without any appropriate security provisions. While some of these concerns do exists in a wired infrastructures and routing protocols and also many counter measures against the malicious attacks [12, 13, 14, 15, 16] are presented as well, but maintaining the physical security of the transmission media is harder in practice with MANETS. Enough security protection is needed to control the disruption of modification of protocol operation. This seams to be somewhat orthogonal to any particular routing protocol approach, e.g. through the application of IP Security techniques.

6) Sleep period operation: Nodes of a MANET will stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods, when the energy conservation or some other need to be inactive. An Adhoc routing protocol should be able to accommodate such sleep periods without any adverse effects. In order to achieve this characteristic it may require a close coupling with the link-layer protocol through a standardized interface.

7) Unidirectional link support: As per the routing algorithms design goes, bidirectional links will functions well than unidirectional links. Sometimes, an enough number of bidirectional links exist so that usage of unidirectional links is of limited added value. However, it is more valuable in certain situations, where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions.

The following list shows some of the quantitative metrics that can be used to measure the performance of any routing protocol [1].

1. End-to-end data throughput and delay: Statistical measures of data routing performance (e.g., means, variances, distributions) are important. These are the measures of a routing policy's effectiveness.
2. Route Acquisition Time: A specific form of external end-to-end delay measurement of particular concern with "on demand" routing algorithms is the time required to establish route(s) when requested.
3. Percentage Out-of-Order Delivery: An external measure of connectionless routing performance of particular interest to transport layer protocols, such as TCP which prefer in-order delivery.

4. Efficiency: If data routing effectiveness is the external measure of a policy's performance, efficiency is the internal measure of its effectiveness. To achieve a given level of data routing performance, two different policies can expend differing amounts of overhead, depending on their internal efficiency. Protocol efficiency may or may not directly affect data routing performance. If control and data traffic must share the same channel, and the channel's capacity is limited, then excessive control traffic often impacts data routing performance. It is useful to track several ratios that illuminate the internal efficiency of a protocol in doing its job:

* Average number of data bits transmitted/data bit delivered-- this can be thought of as a measure of the bit efficiency of delivering data within the network. Indirectly, it also gives the average hop count taken by data packets.

* Average number of control bits transmitted/data bit delivered--this measures the bit efficiency of the protocol in expending control overhead to delivery data. Note that this should include not only the bits in the routing control packets, but also the bits in the header of the data packets. In other words, anything that is not data is control overhead, and should be counted in the control portion of the algorithm.

* Average number of control and data packets transmitted/data packet delivered—rather than measuring pure algorithmic efficiency in terms of bit count, this measure tries to capture a protocol's channel access efficiency, as the cost of channel access is high in contention-based link layers.

In addition, we must also consider with respect to the networking context where in a protocol performance is measured. Different network parameters that vary often according to the applications used include [1]:

- Network size—this is the measurement taken as the number of nodes in the network.
- Network connectivity—this is the measurement of the average degree of a node, in turn gives the average number of neighbours of a node in the network.
- Topological rate of change—this gives the measure of the speed with which a network topology keeps changing.
- Capacity of a link –This is the measure of effective link speed in bits/second, when it accounts for losses due to multiple accesses, coding, framing, etc.
- Unidirectional links—this gives the measure of the effectiveness of a protocol performance as a function of the presence of unidirectional links.
- Traffic patterns—this gives the measure of the effectiveness of a protocol in adapting to dynamic, non-uniform or bursty traffic patterns.
- Mobility—this gives the measure of the different circumstances, to find out whether the temporal and spatial topological correlation relevant to the performance of a routing protocol or not. Thereby it also helps in finding out most appropriate model for simulation of nodes mobility in a MANET.
- Fraction and frequency of sleeping nodes—this gives the measure of the protocol performance in the presence of sleeping and awakening nodes in the network.

When wide range of networking scenarios in MANETS are considered like small, collaborative, ad hoc groups to larger mobile, multihop networks, a protocol should function most effectively over this a wide range of networks. The protocol for MANET should also keep in account of scarcity of bandwidth and energy related constraints and work well.

Finally, MANETS has got several networking opportunities that need to be intrigued. As the engineering tradeoffs are many and challenging for MANETS, a diverse set of performance issues requires new protocols for network control. To help out researchers to measure the

goodness of the network performance, we proposed in this paper an outline of protocol performance issues that highlight performance parameters that will help to promote meaningful comparisons and assessments of protocol performance. This recognizes the suitability of the routing protocol for particular network contexts [1].

6. CONCLUSION

Mobile Ad hoc networks are generally more vulnerable to physical security threats than fixed or hardwired networks. This paper throws a light on different concepts of MANETS that can help researchers to the maximum. Especially when security comes as a major factor of concern for MANETS, we need to study a lot of issues and security considerations. Several link-level security approaches like encryption techniques are often used within wireless networks to reduce the threats. Several authentication schemes have been considered and implemented ranging from a simple shared-key approaches, public key cryptographies based authentication mechanisms to ensure security in MANETS. As an extension work of this, we are proposing a semantic security mechanism in the forthcoming paper to ensure more security for MANETS against network layer attacks.

ACKNOWLEDGEMENTS

The authors would like to thank all nears and dears who have been source of inspiration to her.

REFERENCES

[1] S. Corson and J. Macker, “RFC 2501 - Mobile Ad Hoc Networking (MANET): Routing Protocol Pe”, Network Working Group, Request for Comments: 2501, University of Maryland, Naval Research Laboratory, JAN 1999.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks”, Wireless Communications, IEEE In Wireless Communications, IEEE, Vol. 14, No. 5. (06 December 2007), pp. 85-91.

[3] T. Ciszkowski, Z. Kotulski, “Distributed Reputation Management in Collaborative Environment of Anonymous MANETs”, in Proceedings of International Conference on "Computer as a Tool"EUROCON, Warsaw, 2007, pp. 1028-1033.

[4] Krishna Moorthy Sivalingam, “Tutorial on Mobile Ad Hoc Networks”, 2003.

[5] S Gowrishankar , T G Basavaraju, and Subir Kumar Sarkar, “Effect of Random Mobility Models Pattern in Mobile Ad hoc Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.6, June 2007.

[6] C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Networks, Architectures and Protocols”, Second Edition, Low price Edition, Pearson Education, 2007.

[7] P. Gupta, P.R. Kumar , “Capacity of Wireless Networks”, IEEE Transactions on Information Theory, Vol. 46, No. 2, March 2000.

[8] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris,” Capacity of Ad Hoc Wireless Networks”, In proceedings of IEEE Infocom, April 2001.

[9] M. Grossglauser and D. Tse, “Mobility increases the capacity of ad hoc wireless networks”, IEEE/ACM Transactions on Networking, Vol. 10, No. 4, August 2002.

[10] P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Transactions on Information Theory, Vol. 51, No. 3, Mar 2005, pp. 834-847.

[11] M. Grossglauser, "The capacity of Mobile Ad hoc Networks", In Proceedings of IEEE Infocom, April 2001.

[12] B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks," IEEE GLOBECOM '06.

[13] Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Workshop on Real-World Wireless Sensor Networks, June 20–21, 2005.

[14] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, Vol. 24, No. 2, Feb. 2006.

[15] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," In Proceedings of IEEE International Conference on Network Protocols, Nov. 2002.

[16] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Workshop on Wireless Security, Sept. 2002, pp. 1–10.

Authors

G. S. Mamatha has completed her MTech from Visveswaraya technological University in the year 2004 in the field of Computer Science and Engineering. She is currently pursuing her Ph.D in Avinashi Lingam University for women; Coimbatore. She has 6 Years of academic experience and working as assistant Professor in R.V.C.E. She is a member of ISTE. Her area of research includes Network security, Software Engineering and Multimedia systems.

Dr. S. C. Sharma is Vice-Chancellor of Tumkur University, Tumkur, Karnataka. He pursued PhD in Mechanical Engineering from Mysore University, Doctor of Science in CSE from Kuvempu University, Doctor of Engineering from Avinashi Lingam University. The various positions he held includes as Adjunct Professor Of Engineering in West Virginia University, USA, Senior scientist, University of Wisconsin, Milwaukee, USA, State Government of Karnataka Nominee as Member of Executive Council, Member, Research Review Committee, Associate Editor, Research Journal Editorial Board, Syndicate member, Avinashi Lingam University, Coimbatore, Tamil nadu. His specialization areas include advanced materials, Metal Casting, Internet Enabled Automated System. He has got several Fellowships and awards for his contributions in academics and music field.