Volume-4, Issue-5, October-2014, ISSN No.: 2250-0758
International Journal of Engineering and Management Research
Available at: www.ijemr.net
Page Number: 77-81

Open Performance Issues Along with Security Considerations in MANETs

Aakash Chabaque[1], Dr. Sohan Garg[2]
[1]Research Scholar Swami Vivekanand University, Madhya Pradesh, INDIA
[2]SCRIET- CCS University Campus Meerut, Uttar Pradesh, INDIA

ABSTRACT

This paper first describes the characteristics, applications of Mobile Ad hoc Networks (MANETs), and their idiosyncrasies with respect to traditional, hardwired packet networks. It then discusses the effect these differences have on the design and evaluation of network control protocols with an emphasis on routing performance evaluation considerations.

I. INTRODUCTION

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The 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. Within the Internet community, routing support for mobile hosts is presently being formulated as "mobile IP" technology. This is a technology to support nomadic host "roaming", where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. Supporting this form of host mobility (or nomadicity) requires address management, protocol interoperability enhancements and the like, but core network functions such as hop-by-hop routing still presently rely upon pre-existing routing protocols operating within the fixed network. In contrast, the 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--themselves form the network routing infrastructure in an ad hoc fashion.

II. TYPES OF MANETS:

There are different types of MANETs including:

- In VANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

MANETs Applications:

Some of the typical applications include:

1) Military battlefield: Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.

2) Collaborative work: For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

3) Local level: Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

4) Personal area network and bluetooth : A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

5) Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a

communication network is needed.

III. CHARACTERISTICS OF MANETS

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

MANETs have several salient characteristics

1) Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

2) Bandwidth-constrained: variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.--is often much less than a radio's maximum transmission rate. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

3) Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

4) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

In addition, some envisioned networks (e.g. mobile military networks or highway networks) may be relatively large (e.g. tens or hundreds of nodes per routing area). The need for scalability is not unique to MANETS. However, in light of the preceding characteristics, the mechanisms required to achieve scalability likely are.

These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet.

IV. GOALS OF MANETS:

The intent of the newly formed IETF manet working group is to develop a peer-to-peer mobile routing capability in a purely mobile, wireless domain. This capability will exist beyond the fixed network (as supported by traditional IP networking) and beyond the one-hop fringe of the fixed network.

The near-term goal of the MANET working group is to standardize one (or more) intra-domain unicast routing protocol(s), and related network-layer support technology which:

* provides for effective operation over a wide range of mobile networking "contexts" (a context is a set of characteristics describing a mobile network and its environment);
* supports traditional, connectionless IP service;
* reacts efficiently to topological changes and traffic demands while maintaining effective routing in a mobile networking context.

The working group will also consider issues pertaining to addressing, security, and interaction/interfacing with lower and upper layer protocols. In the longer term, the group may look at the issues of layering more advanced mobility services on top of the initial unicast routing developed. These longer term issues will likely include investigating multicast and QoS extensions for a dynamic, mobile area.

V. CHALLENGES OF MANETS

A Manet environment has to overcome certain issues of limitation and inefficiency. It includes:

- The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The reliability of wireless transmission is resisted by different factors.

- Limited range of wireless transmission – The limited radio band results in reduced data rates compared to the wireless networks. Hence optimal usage of bandwidth is necessary by keeping low overhead as possible.
- Packet losses due to errors in transmission – MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate (BER)), interference, frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and uni-directional links.
- Route changes due to mobility- The dynamic nature of network topology results in frequent path breaks.
- Frequent network partitions- The random movement of nodes often leads to partition of the network. This mostly affects the intermediate nodes.

VI. MANET ROUTING PROTOCOL PERFORMANCE ISSUES

To judge the merit of a routing protocol, one needs metrics--both qualitative and quantitative--with which to measure its suitability and performance. These metrics should be *independent* of any given routing protocol.

The following is a list of desirable qualitative properties of MANET routing protocols:

1) Distributed operation: This is an essential property, but it should be stated nonetheless.

2) Loop-freedom: Not required per se in light of certain quantitative measures (i.e. performance criteria), but generally desirable to avoid problems such as worst-case phenomena, e.g. a small fraction of packets spinning around in the network for arbitrary time periods. Ad hoc solutions such as TTL values can bound 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: Instead of assuming an uniform traffic distribution within the network (and maintaining routing between all nodes at all times), let the routing algorithm adapt to the traffic pattern on a demand or need basis. If this is done intelligently, it can utilize network energy and bandwidth resources more efficiently, at the cost of increased route discovery delay.

4) Proactive operation: The flip-side of demand-based operation. In certain contexts, the additional latency demand-based operation incurs may be unacceptable. If bandwidth and energy resources permit, proactive operation is desirable in these contexts.

5) Security: Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of of the transmission media is harder in practice with MANETs. Sufficient security protection to prohibit disruption of modification of protocol operation is desired. This may be somewhat orthogonal to any particular routing protocol approach, e.g. through the application of IP Security techniques.

6) "Sleep" period operation: As a result of energy conservation, or some other need to be inactive, nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocol should be able to accommodate such sleep periods without overly adverse consequences. This property may require close coupling with the link-layer protocol through a standardized interface.

7) Unidirectional link support: Bidirectional links are typically assumed in the design of routing algorithms, and many algorithms are incapable of functioning properly over unidirectional links.Nevertheless, unidirectional links can and do occur in wireless networks. Oftentimes, a sufficient number of duplex links exist so that usage of unidirectional links is of limited added value. However, in situations where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions, the ability to make use of them is valuable.

Performance Metrics of MANETs Routing Protocols

In the evaluation of routing protocols different performance metrics are used. They show different characteristics of the whole network performance. In this performance comparison we evaluate the Network Load, throughput and End-to-End delay of selected protocols in order to study the effects on the whole network.

Network Load

It is the total load measured in bits/sec, which all higher layers put forward on the WLAN layers in network. It represents the effectiveness of routing protocols when the packets are being received. When there is rush of traffic on the network and it is not easy to manage this is referred as network load. For the best performance it is the quality of network to handle all the traffic in smooth manners so that the deadlock may not occur.

Throughput

Throughput is the ratio of total amounts of data that reaches the receiver from the source to the time taken by the receiver to receive the last packet [27]. It is represented in packets per second or bits per second. In the MANET unreliable communication, limited energy, limited bandwidth and frequent topology change affect throughput [15]. A network requires high throughput and can be represented mathematically by the following equation.

Throughput= (Number of Delivered Packets X Packet Size X Bandwidth) / (Total Simulation Period)

End-to End Delay

The average time taken by the packets to pass through the network is called end-to-end delay. This is the time when a sender generates the packet and it is received

by the application layer of destination, it is represented in seconds. This is the whole time that includes all delay of network such as transmission time, buffer queues, MAC control exchanges and delay produced by routing activities Different applications require different packet delay levels. Low average delay is required in the network of delay sensitive applications like voice. MANET has the characteristics of packet transmissions due to weak signal strengths of nodes, connection make and break, and the node mobility. These are several reasons that increase the delay in the network. Therefore the end-to-end delay is the measure of how a routing protocol accepts the various constraints of network and show the reliability.

Performance Challenges of MANETs Routing Protocols

Security

Mobile ad-hoc networks experience a radio environment that is not dedicated, therefore is not secure posing a security threat to the network stability. As the traffic is relayed through different nodes therefore traditional security measures such as cryptography, interleaver is inefficient to ensure the security. A more robust, generalized security measures for node-to-node / end-to-end security solution needs to be investigated.

Quality of Service (QoS)

Performance characteristics such as jitter, delay, bandwidth, packet loss probability measure the quality of service to be attained. The quality of the link remains varying during the connectivity time of ad-hoc networks, thereby the quality parameters are more difficult to be maintained. Moreover the behavior of the above parameters on different routing protocols is not same. Quality of Service in mobile ad-hoc networks requires integration of vertical-layer or cross-layer. Therefore the means to detect and troubleshoot the artifacts of above mentioned parameters need to be optimized in order to ensure the quality of service to end users.

Scalability

The scalability challenge appears when the performance of routing protocol in ad-hoc network is tested by increasing the network size, open challenge of ad-hoc networks is defined as whether the wider ad-hoc network is capable to give the service that is acceptable. The dynamic environment of wireless ad-hoc network poses big challenge to cater the huge amount of broadcast traffic in change of topology.

Saving Energy

Due to the mobile nature and environmental variations saving the energy of the network has been a desired feature. As the infrastructure in ad-hoc network is not fixed, thereby increasing the overhead data that results in more consumption of transmitted power. The requirement of user that is near the transmitter is different from the requirement of that user who is away from transmitter. Adding diversity increases consumption of power, therefore energy management by optimizing the power consumption is an important performance challenge.

VII. SECURITY CONSIDERATIONS, SECURITY GOALS AND ATTACKS ON MANETS

Mobile wireless networks are generally more prone to physical security threats than are fixed, hardwired networks. Existing link- level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Absent link-level encryption, at the network layer, the most pressing issue is one of inter-router authentication prior to the exchange of network control information. Several levels of authentication ranging from no security (always an option) and simple shared-key approaches, to full public key infrastructure-based authentication mechanisms will be explored by the group. As an adjunct to the working groups efforts, several optional authentication modes may be standardized for use in MANETs.

In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

1)Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

2) Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. Protection of information which is exchanging through a MANET. It should be protected against any disclosure attack like eavesdropping- unauthorized reading of message.

3) Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way.. Integrity assures that a message being transferred is never corrupted.

4) Authentication: Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The recourses of network should be accessed by the authenticated nodes.

5) Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

6) Resilience to attacks: It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

7) Freshness: It ensures that malicious node does not resend previously captured packets.

The application of this wireless network is limited due to the mobile and ad hoc nature. Similarly, the lack of a centralized operation prevents the use of firewall in MANETs. It also faces a multitude of security threats just like wired networks. It includes spoofing, passive eavesdropping, denial of service and many others. The

attacks are usually classified on the basis of employed techniques and the consequences.

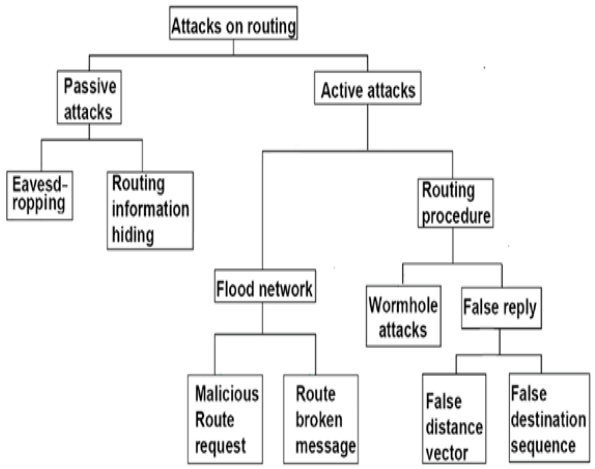

Figure: Security Attacks

REFERENCES

[1] Adamson, B., "Tactical Radio Frequency Communication Requirements for IPng", RFC 1677, August 1994.

[2] X. Hong, M. Gerla, G. Pei, and Ch.-Ch. Chiang; "A group mobility model for ad hoc wireless networks," in ACM/IEEE MSWiM, August 1999.

[3] Z. Chen, H. Kung, and D. Vlah; ''Ad hoc relay wireless networks over moving vehicles on highways,'' in Proc. of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, pp. 247–250, 2001.

[4] Z. Haas; "A New Routing Protocol for Reconfigurable Wireless Networks", Proceedings of the IEEE International Conference on Universal Personal Communications (ICUPC), pages 562–565, October 1997.

[5] I. Chlamtac and A. Lerner, "Link allocation in mobile radio networks with noisy channel",
In IEEE INFOCOM, Bar Harbour. www.openu.ac.il/Personal_sites/anat-lerner.html, FL, April 1986.

[6] I. Chlamtac and A. Lerner, "Fair algorithms for maximal link activiation in multi-hop radio networks", IEEE Transactions on Communications COM-3, Issue-7, Vol. 35, 1987, pp. 739-746.

[7] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou. "A Multi –radio unification protocol for IEEE 802.11 wireless networks". In IEEE International conference on broadband networks, (BroadNets), 2004.

[8] C. Perkins, "Ad hoc Networking," Chapter 4, Addison-Wesley, December 2000.

[9] C. Siva Ram Murthy and B.S. Manoj, "Ad hoc Wireless Networks Architecture and Protocols", Prentice Hall, 2004.

[10] M.S. Corson, S. Batsel and J. Macker, "Architecture consideration for mobile mesh networking", Conference Proceeding, IEEE, Vol.1, 21-24 Oct. 1996, pp. 225-229.

[11] P. Merlin and A. Segall, "A fail safe distributed routing protocol", IEEE Transactions on Communications, COM-27 (9), Sep. 1979, pp. 1280-1287.

[12] J.M. Jaffe and P.H. Moss, "A responsive distributed routing algorithm for computer networks", IEEE Transactions on Communications, COM-30 (7): July 1982, pp. 1758-1762.