Ad Hoc Networks Technical Issues on Radio Links Security & QoS

M.A Siddique[1], Sarah Khan[2], Firaz Noushad[3]

[1]Vijay Rural Engineering College, Dept of Computer Science
Nizamabad-503001, A.P, India,
ahtesham.siddique@gmail.com

[2]Vijay College of Engineering for Women, Dept of Computer Science
Nizamabad-503001, A.P, India,
siddiqui.sarah04@gmail.com

[3]Vijay Rural Engineering College, Dept of Computer Science
Nizamabad-503001, A.P, India,
write2firaz@gmail.com

Abstract: ***Mobile ad hoc networks (MANETS) are self-created and self organized by a collection of mobile nodes, interconnected by multi-hop wireless paths in a strictly peer to peer fashion. Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and centralized administration. Communication in MANET is done via multi-hop paths. Lots of challenges are there in this area, MANET contains diverse resources, the line of defense is very ambiguous, Nodes operate in shared wireless medium, Network topology changes unpredictably and very dynamically, Radio link reliability is an issue, connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET acts a router that forwards data packets to other nodes.***

Keywords*:* Routing Protocols, SRP. QoS, **IEEE** 802.11b, IEEE 802.11g, Bluetooth, (IEEE 802.15.1)

1. Introduction

An ad hoc network is a collection of wireless mobile nodes (or routers) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the Internet. Ultimo, mobility, large network size combined with device heterogeneity, bandwidth, and battery power constraints make the design of adequate routing protocols a major challenge. Some form of routing protocol that may wish to exchange packets might not be able to communicate directly Mobile users will want to communicate in situations in which no fixed wired infrastructure is available. For example, a group of researchers en route to a conference may meet at the airport and need to connect to the wide area network, students may need to interact during a lecture, or firefighters need to connect to an ambulance en route to an emergency scene. In such situations, a collection of mobile hosts with wireless network interfaces may form a temporary network without the aid of any established infrastructure or centralized administration. Because

nowadays many laptops are equipped wit powerful CPUs, large hard disk drives, and good sound and image capabilities, the idea of forming a network among these researchers, students, or members of a rescue team, who can easily be equipped with the devices mentioned above, seems possible. Such networks received considerable attention in recent years in both commercial and military applications, due to the attractive properties of building a network on the fly and not requiring any preplanned infrastructure such as a base station or central controller.

A mobile ad hoc network (MANET) group has been formed within IETF. The primary focus of this working group is to develop and evolve MANET specifications and introduce them to the Internet standard track. The goal is to support mobile ad-hoc networks with hundreds of routers and solve challenges in this kind of network.

Some challenges that ad hoc networking faces are limited wireless transmission range, hidden terminal problems, packet losses due to transmission errors, mobility- induced route changes, and battery constraints. Mobile ad hoc networks could enhance the service area of access networks and provide wireless connectivity into areas with poor or previously no coverage (e.g., cell edges). Connectivity to wire infrastructure will be provided through multiple gateways with possibly different capabilities and utilization.

To improve performance, the mobile host should have the ability to adapt to variation in performance and coverage and to switch gateways when beneficial. To enhance the

prediction of the best overall performance, a network-layer metric has a better overview of the network. Ad hoc networking brings features like easy connection to access networks, dynamic multi hop network structures, and direct peer-to-peer communication. The multi hop property of an ad hoc network needs to be bridged by a gateway to the wired backbone. The gateway must have a network interface on both types of networks and be a part of both the global routing and the local ad hoc routing. Users could benefit from ubiquitous networks in several ways. User mobility enables users to switch between devices, migrate sessions, and still get the same personalized services. Host mobility enables the users' devices to move around the networks and maintain connectivity and reach ability. is in general necessary in such an environment, because two hosts field of wireless and mobile communications has experienced an unprecedented growth during the past decade.

2. Wireless Network Communications (Ad hoc & Cellular)

Wireless communication can be via different media such as ultrasound, infrared or electromagnetic radio waves. Radio waves are the most suitable for LBS as the other media have more problems e.g. with walls and other obstacles. Common wireless networks today can be classified by two means. One classifier is the network range which is also induced by the network's purpose and the physical limitations of radio waves. The other classifier is the networks topology, whether the network consists of a large infrastructure of mostly in-mobile network-nodes and the mobile client's access only the nodes or the clients form an "Ad-Hoc" network by being the nodes themselves. Radio waves do have a limited range. No matter which technologies and thus what ranges can be reached with a wireless radio transmission, for establishing communication between multiple components as a network three strategies are available: cellular infrastructure networks, Ad-Hoc networks and hybrid networks. Ad-Hoc Networks Opposed to infrastructure wireless networks, where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET, does not rely on a fixed infrastructure for its operation.

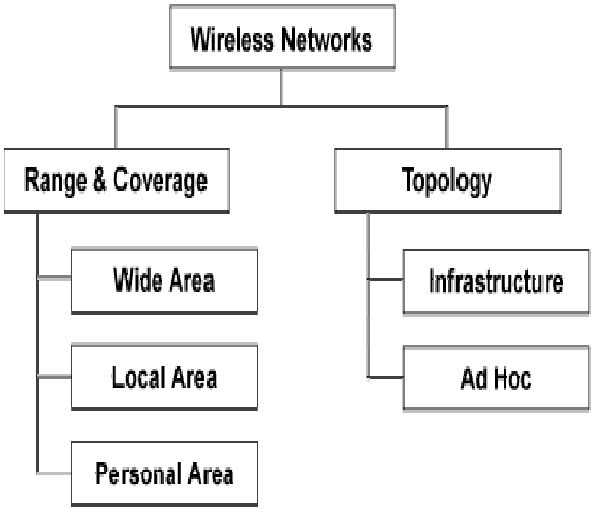

Figure 1: Classification of Wireless Networks

The network is an autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's send range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. These nodes are often energy constrained that is, battery-powered devices with a great diversity in their capabilities. Furthermore, devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. In this energy-constrained, dynamic, distributed multi-hop environment, nodes need to organize themselves dynamically in order to provide the necessary network functionality in the absence of fixed infrastructure or central administration. The specific characteristics and complexities impose many design challenges to the network protocols. In addition, these networks are faced with the traditional problems inherent to wireless communications such as lower reliability than wired media, limited physical security, time varying channels, interference, etc. Despite the many design constraints, mobile ad hoc networks offer numerous advantages. First of all, this type of network is highly suited for use in situations where a fixed infrastructure is not available, not trusted, too expensive or unreliable. Because of their self-creating, self-organizing and self-administering capabilities, ad hoc networks can be rapidly deployed with minimum user intervention. There is no need for detailed planning of base station installation or wiring. Also, ad hoc networks do not need to operate in a stand-alone fashion, but can be attached to the Internet, thereby integrating many different devices and making their services available to other users. Furthermore, capacity, range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity. As a consequence, mobile ad hoc networks are expected to become an important part

of the future 4G architecture, which aims to provide pervasive computer environments that support users in accomplishing their tasks, accessing information and communicating anytime, anywhere and from any device.

3. Mobile Ad-hoc Network Applications

Ad hoc networks are key to the evolution of wireless networks.. Ad hoc networks are typically composed of equal nodes that communicate over wireless links without any central control. Although military tactical communication is still considered the primary application for ad hoc networks, commercial interest in this type of networks continues to grow. Applications such as rescue missions in times of natural disasters, law enforcement operations, commercial and educational use, and sensor network are just a few possible commercial examples.

Ad hoc wireless networks inherit the traditional problems of wireless and mobile communications, such as bandwidth optimization, power control, and transmission quality enhancement. In addition, the multi hop nature and the lack of fixed infrastructure generates new research problems such as configuration advertising, discovery, and maintenance, as well as ad hoc addressing and self-routing

- Tactical networks: Military communication and operations, automated battlefields
- Disaster services: Search and rescue operations, Disaster recovery, Replacement of fixed infrastructure in case of environmental disasters, Policing and fire fighting, Supporting doctors and nurses in hospitals
- Commercial and civilian: E-commerce, electronic payments anytime and anywhere environments.
- Home and enterprise: Home/office wireless networking, Conferences, meeting rooms, Personal area networks (PAN), Personal networks (PN), Networks at construction sites.
- Education: Universities and campus settings, Virtual classrooms, Ad hoc communications during meetings or lectures.
- Entertainment: Multi-user games, Wireless P2P networking, Outdoor Internet access, Robotic pets, Theme park Sensor networks.
- Home applications: smart sensors & actuators embedded in consumer electronics, Body area network (BAN) Data tracking of environmental conditions, animal movements, chemical / biological detection.
- Context aware services: Follow-on services: call forwarding, mobile workspace.

4. Security issues & Challenges

Security has become a primary concern to provide protected communication between mobile nodes in a hostile environment. Unlike the wired line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multi fence security solutions that achieve both broad protection and desirable network performance. One of the fundamental vulnerabilities of MANETs comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well-defined place or infrastructure where we may deploy a single security solution. Moreover, portable devices, as well as the system security information they store, are vulnerable to compromises or physical capture, especially low-end devices with weak protection.

Attackers may sneak into the network through these subverted nodes, which pose the weakest link and incur a domino effect of security breaches in the system. The stringent resource constraints in MANETs constitute another nontrivial challenge to security design. The wireless channel is bandwidth constrained and shared among multiple networking entities. The computation capability of a mobile node is also constrained. For example, some low-end devices, such as PDAs, can hardly perform computation-intensive tasks like asymmetric cryptographic computation. Because mobile devices are typically powered by batteries, they may have very limited energy resources. The wireless medium and node mobility pose far more dynamics in MANETs compared to the wired line networks. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network on their own will. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Despite such dynamics, mobile users may request “anytime, anywhere” security services as they move from one place to another. The above characteristics of MANETs clearly make a case for building multi fence security solutions that achieve both broad protection and desirable network performance.

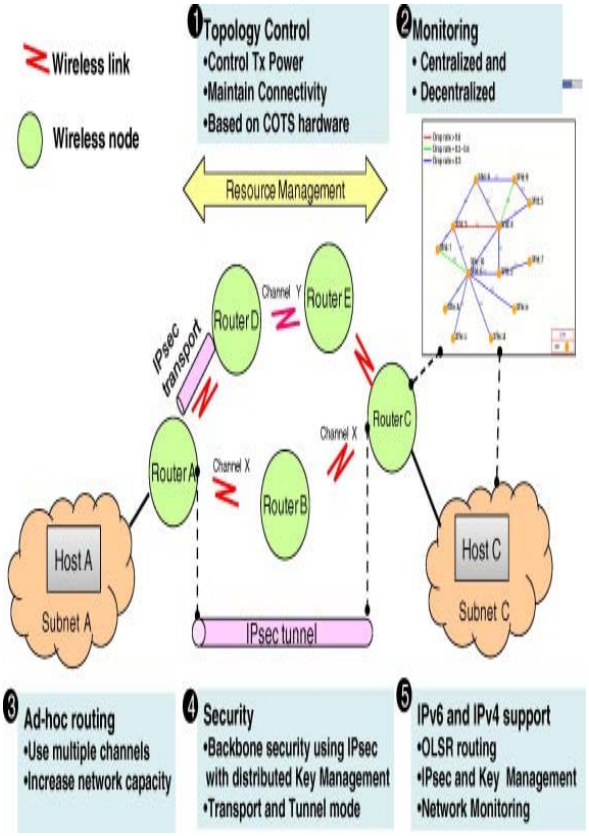

Figure 2: Transmission using Wireless Link

First, the security solution should spread across many individual components and rely on their collective protection power to secure the entire network. The security scheme adopted by each device has to work within its own resource limitations in terms of computation capability, memory, communication capacity, and energy supply. Second, the security solution should span different layers of the protocol stack, with each layer contributing to a line of defense. No single-layer solutions possible to thwart all potential attacks. Third, the security solution should thwart threats from both outsiders who launch attacks on the wireless channel and network topology, and insiders who sneak into the system through compromised devices and gain access to certain system knowledge. Fourth, the security solution should encompass all three components of prevention, detection, and reaction that work in concert to guard the system from collapse. Finally, the security solution should be practical and affordable in a highly dynamic and resource-constrained networking scenario.

There are three types of routing protocols: Proactive Protocols, Reactive Protocols and Hybrid Protocols. Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency.

Security at Data-Link Layer: The wireless medium access protocol implements mechanisms based on cryptography to avoid unauthorized access and to enhance the privacy on radio links. An analysis of IEEE 802.11 and Bluetooth can be discussed in brief. Security in the IEEE 802.11 standard is provided by the Wired Equivalent Privacy (WEP) scheme, which supports both data encryption and integrity. The key is a 40-bit secret key and is shared only by all the devices of a WLAN, or is a pair wise secret key shared only by two communicating devices. Bluetooth uses cryptographic security mechanisms implemented in the data link layer. A key management service provides each device with a set of symmetric cryptographic keys required for the initialization of a secret channel with another device, the execution of an authentication protocol, and the exchange of encrypted data on the secret channel.

Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, fabricating false routing information, and impersonating other nodes. The Secure Routing Protocol (SRP) is an extension that is applied to several existing reactive routing protocols. SRP is based on the assumption of the existence of a security association between the sender and receiver based on a shared secret key negotiated at the connection setup. SRP fights against the attacks that disrupt the route discovery process. A node initiating a route discovery is able to identify and discard false routing information. Ariadne is a secure ad-hoc routing protocol based on DSR and the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) authentication protocol. The Authenticated Routing for Ad Hoc Network (ARAN) Protocol is on-demand, secure, and detects and protects against malicious actions carried out by third parties in the ad hoc environment. ARAN is based on certificates from a trusted certificate server before joining the ad hoc network. Secure Efficient Ad Hoc Distance (SEAD) is a proactive secure routing protocol based on routing table update messages. The basic idea is to authenticate the sequence number and the metric field of a routing table update message using one-way hash functions. Hash chains and digital signatures are used by the Secure Ad Hoc On-Demand Distance Vector (SAODV) mechanism.

Quality of Service (QoS): The ability of a network to provide QoS depends on the intrinsic characteristics of all the network components, from transmission links to MAC and network layers. Wireless links have a low and highly variable capacity, and high loss rates. Topologies are highly dynamic and have high packet loss rates. Random access– based MAC protocols have no QoS support. QoS MAC protocols solve the problems of medium contention, support reliable unicast communications, and provide resource reservation for real-time traffic in a distributed wireless environment. Numerous MAC protocols and improvements that have proposed protocols that can provide QoS guarantees to real-time traffic in a distributed wireless environment include Group Allocation Multiple

Access with Piggyback Reservation (GAMA/PR) protocol and Black Burst (BB) contention mechanism.

With the rapid development of Internet technology, when people for the Best effort service is no longer satisfied, how to get more bandwidth, how to reduce the mistakes, how to reduce the delay phenomenon, making Quality of Service (QoS) related research, including the Integrated Service (RSVP), Differentiated Service, etc., has become an important research topic. In the above-mentioned several agreements, most of them are made in the last two years, only for the basic mode of operation be defined, there is no consideration of QoS, only the ABR (Associativity Based Routing), SSR (Signal Stability Routing) and CEDAR (Core –Extracted Distributed Ad hoc Routing) and so there are three kinds of QoS-related functions. By ABR, for example, ABR defined by the concept of associability is that QoS can be used to indicate a link between adjacent nodes stability, while the adjacent node in the exchange of messages, you can also Bandwidth, Delay and other conditions to join, this way then when you select a path, you can have more choices, but also can do according to the different applications of different considerations to select the most appropriate path may be to ensure a minimum bandwidth that can be used, or between two points of a finite delay. However, in the MANET, the network patterns change at any time, each node may change at any time position, that is, each node is the relationship with the adjacent node may change at any time, therefore, means that the need to provide QoS dependent on regular Beaconing, so that each node to master the situation around in order to provide effective QoS information. Beaconing make the overhead on the network increased, when the node mobility to improve even when the general information that may affect the transmission, which will be in the Ad Hoc Network to provide QoS, the biggest problem.

5. Networking Enhancements for Router Radio Links in MANET

Mobile Ad Hoc Networking (MANET) enhancements address several of the issues faced when merging IP routing and mobile radio communications in ad hoc networking applications. In a MANET, highly mobile "nodes" communicate with each other across bandwidth-constrained radio links. An individual node includes both a radio and a network router, with the two devices interconnected via Ethernet. Key challenges in a MANET environment include:

Convergence: since nodes can rapidly join or leave the network, MANET routing topologies are highly dynamic. Fast convergence in a MANET becomes a challenge because a node's state can change well before the event is detected by the routing protocol's normal timing mechanisms.

Route Selection: Radio link quality in a MANET can vary dramatically due to a variety of factors such as noise, fading, interference, and power fluctuation. As a result, routers need the ability to factor these fluctuations into "best path" selection. Radios have limited buffering capabilities, and could be easily over-loaded with IP traffic. Directional radios that operate on a narrow beam tend to model the network as a series of physical point-to-point connections with neighbor nodes. This point-to-point model does not translate gracefully to multi-hop, multipoint router environments, as it increases the size of each router's topology database and reduces routing efficiency when mobile nodes join and leave the network, based on neighbor up/down signaling from the radio. This feature enables a router to use Layer 2 feedback from its partner radio to optimize Layer 3 processing. Intra-nodal communications between router and radio are supported by means of PPP-over-Ethernet (PPPoE) sessions. A PPPoE session is established between router and its partner radio on behalf of every other router/radio neighbor located in the MANET. Once the PPPoE sessions are established, a PPP session is established end to end. These Layer 2 sessions are the means by which radio network status gets reported to the router's Layer 3 processes. MANET enhancements provide several new capabilities for optimizing routing in a wireless, ad hoc environment:

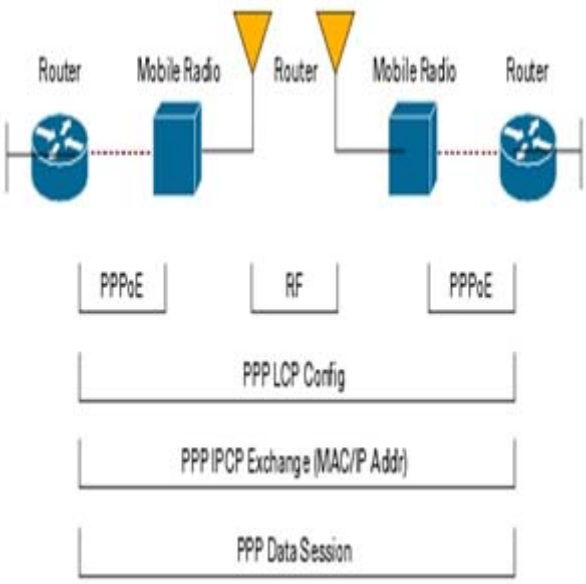

Figure 3: Radio Router Links in MANET

6. Conclusion

The rapid evolution in the field of mobile computing is driving a new alternative way for mobile communication, in which mobile devices form a self-creating, self-organizing and self-administering wireless network, called a mobile ad hoc network.. The development of ad hoc wireless networks and sensor networks provides tremendous opportunities in many areas including disaster recovery, defense, health care, academic, and industrial

environments. However, there are many challenges that need to be addressed as well. The challenges include developing the following: mechanisms for efficient use of limited bandwidth and communication capacity, mechanisms for reducing power consumption and hence extending the battery life, smaller but more powerful mobile devices, algorithms for enhancing information security, and efficient routing procedures. These are major challenges to overcome, but steady progress is being made to address these.

7. Future Scope

There are currently two types of mobile wireless networks. The first is known as infrastructure networks, such as networks with fixed and wired gateways. The bridges for these networks are known as base stations. The second type of wireless network is the mobile ad-hoc network. Ad-hoc connectivity is based on peer-to-peer communication. Future mobile ad-hoc networks will use mobile routers to provide Internet connectivity to mobile ad-hoc users. A mobile router will also allow mobility of an ad-hoc network, where mobile users may use an Internet access within an ad-hoc network domain. Recently, organizations have begun to see potential for such dynamic networks. Mobile ad-hoc networks are of increasing interest for a distributed set of applications, such as distributed collaborative computing, distributed sensing networks, potential fourth generation wireless systems, and response to incidents that destroyed the existing communication structure.

Acknowledgment

The Authors are thankful to there college management authorities, thankful to there parents for their love & affection, Author is thankful to her daughter for her immense love.

References

[1] IEEE 802.11e/D4.4, Draft Supplement to Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC)
[2] Enhancements for Quality of Service (QoS), June 2003. S. Adroutselli-Theotokis and Spinellis. A survey of peer-to-peer content distribution technologies. ACM Computing Surveys, Dec. 2004.
[3] D. Wu and R. Negi. Effective capacity: a wireless link model for support of quality of service. IEEE Transactions on Wireless Communications, 2(4):630–643, 2003
[4] Irshad Ullah, Shoaib Ur, “Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols.”, Master Thesis at School of Computing, Blekinge Institute of Technology, 2009
[5] Suresh Singh Candy Yiu, ``Putting the cart before the horse: merging traffic for energy conservation", IEEE Communications Magazine, June 2011, pp. 78 - 82.
[6] J. Jubin and J.D. Tornow, “The DARPA Packet Radio Network Protocols”, proceedings of the IEEE.

Authors Profile

MA.Siddique, M.TECH(CSE), Associate Professor, Dept of CSE, Vijay Rural Engineering College, Nizambad (Dist), A.P, India. He is author of five research papers, with five papers in international conferences & international journals, His area of interest is in “Ad-hoc networking, wireless communications”.

Sarah Khan, M.TECH (Computer Science), Associate Professor, Dept of CSE, Vijay college of engineering for women, Nizamabad (Dist), A.P, India. She is author of five research papers, with five papers in international conferences & international journals, her area of interest is in “Ad-hoc networking, wireless communications”.

Firaz Noushad, MTECH (CSE), Assistant Professor, Dept of CSE, Vijay Rural Engineering College, Nizamabad (Dist), A.P, India. His area of interest is on MANET Security Issues.