Mobile Ad hoc Network

R. Marutha Veni[1], R. Latha[2]

[1]Dr. SNS Rajalakshmi College of arts and science,
Saravanampatti, Coimbatore – 49, India
maruthaveni12@gmail.com

[2]Dr. SNS Rajalakshmi College of arts and science,
Saravanampatti, Coimbatore – 49, India
lathamani16@gmail.com

Abstract: ***A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing.***

Keywords: Mobile ad hoc networks, Security, Classifications, Highly Dynamic networks.

1. Introduction

Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure.

With the widespread rapid development of computers and the wireless communication, the mobile computing has already become the field of computer communications in high-profile link. Mobile Ad Hoc Network (MANET) is a completely wireless connectivity through the nodes constructed by the actions of the network, which usually has a dynamic shape and a limited bandwidth and other features, network members may be inside the laptop, Personal Digital Assistant (PDA), mobile phones, MP3 players, and digital cameras and so on.

The growth of laptops and 802.11 Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

2. Review of Literature

Security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. In this paper, we focus on fundamental security attacks in Mobile ad hoc networks.

MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. However, these solution are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. MANET can operate in isolation or in coordination with a wired infrastructure, often through a gateway node participating in both networks for traffic relay. This flexibility, along with their self-organizing capabilities, is some of MANET's biggest strengths, as well as their biggest security weaknesses. In this paper different routing attacks, such as active (flooding, black hole, spoofing, and wormhole) and passive (eavesdropping, traffic monitoring, and traffic analysis) are described.

3. Existing Work of Mobile Ad hoc Network

Advances in wireless local-area network technology and the growing interest in public safety communications have created new demands for reliable transmission of real-time multimedia information over distributed mobile ad hoc networks (MANET). Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol (RMP)
- Proactive MANET Protocol (PMP)

If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be

supported. Routing security requirements and issues will also be addressed.

The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best effort multicast forwarding function. The use of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues.

The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing research topics related to MANET environments.

4. Problem Definition

Mobile ad hoc networks are communication networks built up of a collection of mobile devices which can communicate through wireless connections. Mobile ad hoc networks have many challenges such as routing, which is the task of directing data packets from a source node to a given destination. This task is particularly hard in mobile ad hoc networks: due to the mobility of the network elements and the lack of central control, robustness and adaptability in routing algorithms and work in a decentralized and self organizing way. Through the principles of systems architecting and engineering, the problem statement in mobile ad hoc networks could be defined more specifically and accurately. The uncertainties and techniques for mitigating and even taking positive advantages of them can be achieved through a framework of uncertainties.

The systems methodology framework called total systems intervention (TSI) described by Flood and Jackson select a systems methodology for mobile ad hoc networks. The purpose of this paper is to show how TSI when integrated with a framework created to understand the risks and opportunities can help develop strategies to minimize the risks and to take advantage of the opportunities for facing challenges in mobile ad hoc networks.

5. Approaches to Mobile Ad hoc Network

In static networks, network administrators or technicians decide which computer is reached via which way or cable. As radio networks undergo constant changes and low participation-thresholds are a vital part of the “Freifunk”-networks' foundation this task has to be automated as far as possible.

On a regular basis, every node sends out a so called “broadcast” (a general message to all) thereby informing all its neighbors about its existence. The neighbors then relay this message to their neighbors and so on and so forth. This carries the information to every node in the network.

Version one:
In the first phase, the routing algorithm was implemented and tested for its practicality and suitability for the task at hand. For the sending and receiving of originator-messages (information about existence) the UDP port 1966 was chosen.

Version two:
The version one algorithm made a significant assumption: As soon as a node receives existence data from another node, it assumes it can also send data back. In radio networks however, it may very well be that only one-way communication is possible. A mechanism was incorporated into the protocol to allow for this and to solve the arising problems. The mechanism enables the node to determine whether a neighboring node provides bidirectional communication, only bidirectional nodes being considered part of the network, one-way nodes are no longer fully included.

Version three:
The greatest innovation in this version is B.A.T.M.A.N.'s support of multiple network devices. Now a computer or router running B.A.T.M.A.N can be deployed on a central point, like a church or another high building, and have several wired or wireless network interfaces attached to it. When so deployed,

B.A.T.M.A.N can relay network data in more than one direction without any retransmission delay.

Certain unusual phenomena and special circumstances could appear during the determination of the best route through the network. These have been tackled and counteracted to prevent circular routing (which can prevent data reaching its destination) from occurring.

A node can now inform the network that it provides access to the Internet. Other nodes use that information to evaluate whether there is a connection to the Internet close to them and what bandwidth is available.

They can either use a specific gateway or allow B.A.T.M.A.N to determine which gateway to use, based on criteria such as connection speed.

6. Types of MANET

1. VANETs
2. iMANET

1. Vehicular Ad-hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment
2. Internet Based Mobile Ad-hoc Networks (iMANET) are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly.

7. Simulation of MANETs

There are several ways to study MANETs. One solution is the use of simulation tools like OPNET, NetSim and NS2.

8. Security of MANETs

A lot of research was done in the past but the most significant contributions were the PGP (Pretty Good Privacy) and the trust based security but none of the protocols made a decent tradeoff between security and performance. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols.

9. List of Ad Hoc Routing Protocols

An **ad-hoc routing protocol** is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network . In *ad-hoc networks*, nodes are not familiar with the topology of their networks. Instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

Note that in a wider sense, **ad hoc protocol** can also be used literally, that is, to mean an improvised and often impromptu protocol established for a specific purpose.

- Table-driven (Pro-active) routing
- On Demand (Reactive) routing
- Flow-oriented routing
- Hybrid (both pro-active and reactive) routing
- Hierarchical Routing Protocols

9.1 Table-driven (Pro-active) routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

Examples of pro-active algorithms are

- B.A.T.M.A.N.–Better approach to mobile ad hoc networking.
- OLSR Optimized Link State Routing Protocol

9.2 On Demand (Reactive) routing

This type of protocols finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.

Examples of on demand algorithms are

- Admission Control enabled On demand Routing (ACOR)
- Ad hoc On-demand Distance Vector(AODV)
- Dynamic Source Routing
- Dynamic Magnet On-demand Routing
- Power-Aware DSR-based

9.3 Flow-oriented routing

This type of protocols finds a route on demand by following present flows. One option is to uncast consecutively when forwarding data while promoting a new link. The main disadvantages of such algorithms are

1. Takes long time when exploring new routes without a prior knowledge.
2. May refer to entitative existing traffic to compensate for missing knowledge on routes.

Examples of flow oriented algorithms are

- IERP (Interzone Routing Protocol/reactive part of the ZRP)
- RDMAR (Relative-Distance Micro-discovery Ad hoc Routing protocol)

9.4 Hybrid (both pro-active and reactive) routing

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are

1. Advantage depends on number of Mathavan nodes activated.
2. Reaction to traffic demand depends on gradient of traffic volume.

Examples of hybrid algorithms are

- ZRP (Zone Routing Protocol) ZRP uses IARP as pro-active and IERP as reactive component.

9.5 Hierarchical Routing Protocols

With this type of protocols the choice of proactive and of reactive routing depends on the hierarchic level where a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attributation for respective levels. The main disadvantages of such algorithms are

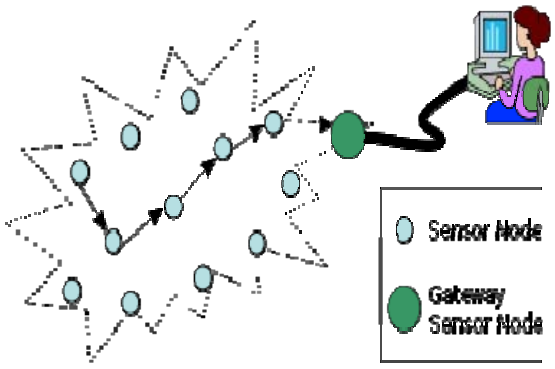
1. Advantage depends on depth of nesting and addressing scheme.
2. Reaction to traffic demand depends on meshing parameters.

Examples of hierarchical routing algorithms are

- CBRP (Cluster Based Routing Protocol)
- FSR (Fisheye State Routing protocol)

10. Wireless Sensor Network

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.



The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network.

11. Wireless Community Networks or Wireless Community Projects

The organizations that attempt to take a grassroots approach to providing a viable alternative to municipal wireless networks for consumers.

Because of evolving technology and locales, there are at least four different types of solution:

- Cluster: Advocacy groups which simply encourage sharing of unmetered internet bandwidth via Wi-Fi, may also index nodes, suggest uniform SSID (for low-quality roaming), supply equipment, DNS services, etc.
- Mesh: Technology groups which coordinate building a mesh network to provide Wi-Fi access to the internet
- WISP: A mesh that forwards all traffic back to consolidated link aggregation point(s) that have centralized access to the internet
- WUG: A wireless user group runs by wireless enthusiasts.

An open network not used for the reselling of internet. Running a combination of various off the shelf WIFI hardware running in the license free ISM bands 2.4 GHz/5.8 GHz

Certain countries regulate the selling of internet access, requiring a license to sell internet access over a wireless network. In South Africa it is regulated by the Independent Communications Authority of South Africa (ICASA). They require that WISP's apply for a VANS or ECNS/ECS license before being allowed to resell internet access over a wireless link.

The cluster and mesh approaches are more common but rely primarily on the sharing of unmetered residential and business DSL and cable Internet. This sort of usage might be non-compliant with the Terms of Service (ToS) of the typical local providers that deliver their service via the consumer phone and cable duopoly. Wireless community network sometimes advocate complete freedom from censorship, and this position may be at odds with the Acceptable Use Policies of some commercial services used. Some ISPs do allow sharing or reselling of bandwidth.

12. Wireless Mesh Network (Wmn)

It is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network.

A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. The animation below illustrates how wireless mesh networks can self form and self heal. Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type.

A wireless mesh network can be seen as a special type of wireless ad-hoc network. A wireless mesh network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area. An ad-hoc network, on the other hand, is formed ad hoc when wireless devices come within communication range of each other. The mesh routers may

be mobile, and be moved according to specific demands arising in the network. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an ad-hoc network, since these nodes are often constrained by resources.

13. Delay-Tolerant Networking (Dtn)

It is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space.

Recently, the term **disruption-tolerant networking** has gained currency in the United States due to support from DARPA, which has funded many DTN projects. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise.

Routing

The ability to transport, or route, data from a source to a destination is a fundamental ability all communication networks must have. Delay and disruption-tolerant networks (DTNs), are characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths. In these challenging environments, popular ad hoc routing protocols such as AODV and DSR [3] fail to establish routes. This is due to these protocols trying to first establish a complete route and then, after the route has been established, forward the actual data. However, when instantaneous end-to-end paths are difficult or impossible to establish, routing protocols must take to a "store and forward" approach, where data is incrementally moved and stored throughout the network in hopes that it will eventually reach its destination.

A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination. This is feasible only on networks with large amounts of local storage and inter node bandwidth relative to the expected traffic. In many common problem spaces, this inefficiency is outweighed by the increased efficiency and shortened delivery times made possible by taking maximum advantage of available unscheduled forwarding opportunities. In others, where available storage and inter node throughput opportunities are more tightly constrained, a more discriminate algorithm is required.

Bundle protocols

In efforts to provide a shared framework for algorithm and application development in DTNs, RFC 4838 and RFC 5050 were published in 2007 to define a common abstraction to software running on disrupted networks. Commonly known as the Bundle Protocol, this protocol defines a series of contiguous data blocks as a bundle—where each bundle contains enough semantic information to allow the application to make progress where an individual block may not. Bundles are routed in a store and forward manner between participating nodes over varied network transport technologies (including both IP and non-IP based transports).

The transport layers carrying the bundles across their local networks are called *bundle convergence layers.* The bundle architecture therefore operates as an overlay network, providing a new naming architecture based on Endpoint Identifiers (EIDs) and coarse-grained class of service offerings.
Protocols using bundling must leverage application-level preferences for sending bundles across a network.

Due to the store and forward nature of delay-tolerant protocols, routing solutions for delay-tolerant networks can benefit from exposure to application-layer information.

For example, network scheduling can be influenced if application data must be received in its entirety, quickly, or without variation in packet delay. Bundle protocols collect application data into bundles that can be sent across heterogeneous network configurations with high-level service guarantees.

The service guarantees are generally set by the application level, and the RFC 5050 Bundle Protocol specification includes "bulk", "normal", and "expedited" markings.

14. Conclusion

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of **Mobile Ad Hoc Networks**.

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

15. Future Scope

In conclusion, wireless networks can be deployed in either infrastructure-based mode or on an ad-hoc basis. Although work is being done and prototype protocols are available for experiments, mobile ad-hoc networks still have difficulties. While some basic network control functions and routing procedures have been developed, many other issues require attention. Rapidly changing topology, network partitions, higher error rates, collision interference, bandwidth constraints, and power limitations together pose new challenges in network control; especially in the design of

higher level protocols for routing and in implementing applications with quality of service requirements.

References

[1] RFC Draft: Better Approach to Mobile Ad-hoc Networking (B.A.T.M.A.N.) - draft-wunderlich-openmesh-manet-routing-00, A. Neumann, C. Aichele, M. Lindner, S. Wunderlich, 07. April 2008

[2] Chakeres and C. Perkins: Dynamic MANET On-demand Routing Protocol (DYMO), Internet Draft, work in progress, June 2008.

[3] Zygmunt J. Haas, Marc R. Pearlman, Prince Samar: The Interzone Routing Protocol (IERP) for Ad Hoc Networks, Internet Draft, work in progress, July 2002.

[4] G. Aggelou, R. Tafazolli: Relative Distance Micro-discovery Ad Hoc Routing (RDMAR) protocol, Internet Draft, work in progress, September 1999.

[5] Perkins, C.; Royer, E. (1999), "Ad-hoc on-demand distance vector routing", The Second IEEE Workshop on Mobile Computing Systems and Applications

[6] C. Perkins and E Royer, “Ad Hoc On-Demand Distance Vector Routing,” 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[7] Toh. C.K., 2002. Ad Hoc Mobile Wireless Networks Protocols and Systems. Prentice Hall,Inc

[8] M. Frodigh, P. Johansson, and P. Larsson. “Wireless ad hoc networking: the art of networking without a network,” Ericsson Review, No.4, 2000, pp. 248-263.

[9] Belding-Royer,E.M. and C.K. Toh,1999. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communication magazine pp: 46-55.

[10] Ad Hoc Networking Extended Research Project. Online Project.http://triton.cc.gatech.edu/ubicomp/505