Survey of Wireless MANET Application in Battlefield Operations

Dr. C. Rajabhushanam and Dr. A. Kathirvel
Department of Computer Science & Engineering
Tagore Engineering College
Chennai, India
rajcheruk@gmail.com, kathir.tagore@gmail.com

***Abstract*—In this paper, we present a framework for performance analysis of wireless MANET in combat/battle field environment. The framework uses a cross-layer design approach where four different kinds of routing protocols are compared and evaluated in the area of security operations. The resulting scenarios are then carried out in a simulation environment using NS-2 simulator. Research efforts also focus on issues such as Quality of Service (QoS), energy efficiency, and security, which already exist in the wired networks and are worsened in MANET. This paper examines the routing protocols and their newest improvements. Classification of routing protocols by source routing and hop-by-hop routing are described in detail and four major categories of state routing are elaborated and compared. We will discuss the metrics used to evaluate these protocols and highlight the essential problems in the evaluation process itself. The results would show better performance with respect to the performance parameters such as network throughput, end-to-end delay and routing overhead when compared to the network architecture which uses a standard routing protocol. Due to the nature of node distribution the performance measure of path reliability which distinguishes ad hoc networks from other types of networks in battlefield conditions, is given more significance in our research work.**

***Keywords*- MANET; routing; protocols; wireless; simulation**

I. Introduction

As the importance of computers in our daily life increases it also sets new demands for connectivity. Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting to the Internet, reading and sending E-mail messages, changing information in a meeting and so on. There are solutions to these needs, one being wireless local area network that is based on IEEE 802.11 standard. However, there is increasing need for connectivity in situations where there is no base station (i.e. backbone connection) available (for example two or more PDAs need to be connected). This is where ad hoc networks step in.

A. AD-HOC NETWORK

The "Ad Hoc Networks" are wireless networks characterized by the absence of fixed infrastructures. This allows the use of this kind of network in special circumstances, such as disastrous events, the reduction or elimination of the wiring costs and the exchange of information among users independently from the environment. The devices belonging to the network must be able not only to transmit and receive data, but also to manage all the functions of the network in a distributed way, as routing of the packets, security, Quality Of Service (QoS), etc; so these are not only terminals, but they become sheer nodes. These devices have a wireless interface and are usually in mobile systems of several types, from those simple ones like PDA to notebooks.

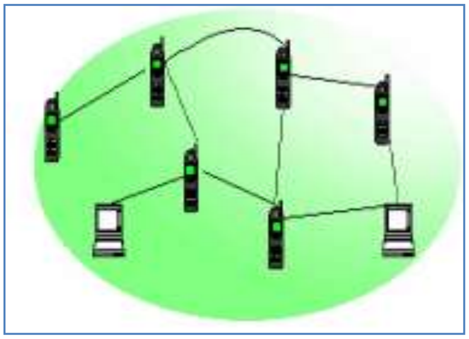

Figure 1. Example of a wireless MANET

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. There are several applications of mobile ad hoc networks such as disaster recovery operations, battle field communications, data sharing in conference halls, etc [1].One of the main issues in such networks is performance- in a dynamically changing topology; the nodes are expected to be power-aware due to the bandwidth constrained network. Another issue in such networks is security - The goals of confidentiality, integrity, authenticity, availability and non-repudiability are very difficult to achieve in MANETs since every node participates in the operation of the network equally and malicious nodes are difficult to detect. The addition of security layers also adds to the performance overhead drastically. We investigate these related issues and study the tradeoffs involved so that an optimal solution may be achieved.

In Latin, ad hoc means "for this," further meaning "for this purpose only”- It is a good and emblematic description of the idea why ad hoc networks are needed. They can be set up anywhere without any need for external infrastructure (like wires or base stations). They are often mobile and that's why a term MANET is often used when talking about Mobile Ad hoc NETworks [2]. MANETs are often defined as follows: A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links - the union of which forms an arbitrary graph. 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 standalone fashion, or may be connected to the larger Internet. The strength of the connection can change rapidly in time or even disappear completely. Nodes can appear, disappear and re-appear as the time goes on and all the time the network connections should work between the nodes that are part of it. As one can easily imagine, the situation in ad hoc networks with respect to ensuring connectivity and robustness is much more demanding than in the wired case [1].

Ad hoc networks are networks are not (necessarily) connected to any static (i.e. wired) infrastructure. An ad-hoc network is a LAN or other small network, especially one with wireless connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.

The ad hoc network is a communication network without a pre-existing network infrastructure. In cellular networks, there is a network infrastructure represented by the base-stations, Radio network controllers, etc. In ad hoc networks every communication terminal (or radio terminal RT) communicates with its partner to perform peer to peer communication. If the required RT is not a neighbor to the initiated call RT, (outside the coverage area of the RT) then the other intermediate RTs are used to perform the communication link. This is called multi-hop peer to peer communication. This collaboration between the RTs is very important in the ad hoc networks. In ad hoc networks all the communication network protocols should be distributed throughout the communication terminals (i.e. the communication terminals should be independent and highly cooperative).

In wireless communication, Ad hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. In order to facilitate communication within the network, a routing protocol is used to discover have been proposed for MANET and some of them have been widely used. This project paper utilizes network scoping to model MANET routing for four different routing protocols: Dynamic Source Routing (DSR), Ad hoc on-demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) and Location Aided Routing (LAR) and compare them with the traditional mathematical equation models [1].

B. *Application Areas*

Some of the applications of MANETs are

- Military or police exercises.
- Disaster relief operations.
- Mine site operations.
- Urgent Business meetings
- Personal area network

Such networks can be used to enable next generation of battlefield applications envisioned by the military including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. Ad Hoc networks can provide communication for civilian applications, such as disaster recovery and message exchanges among medical and security personnel involved in rescue missions.

Many examples of MANETs can be found in real life where an access point and existing infrastructure is not available. For example, battlefields and emergencies where no one has the time to establish access points are the prime examples of MANETs. Common examples are:

Battlefield situations where each jeep and even each soldiers gun has a wireless card. These “nodes” form a MANET and communicate with each other in the battlefield. In addition, MANETs can be used to detect hostile movements in remote areas instead of land mines.

Emergency situations where, for example, a building has been destroyed due to fire, earthquake, or bombs. In such a case, it is important to set up a quick network. MANETs are ideal for such situations. For example, in emergency operation, police and fire fighters can communicate through a MANET and perform their operations without adequate wireless coverage.

II. Previous Work

Most of the previous work have reviewed and implemented the vast literature using various routing protocols employing the constant bit rate for their analysis [3], [4]. Most of the previous is limited on performing simulations for ad hoc networks. Our work differs in that we use variable bit ratio in a combat situation with battlefield like conditions. We will observe and comment on the behavior of each protocol.

A. *Routing protocols and Algorithm*

An ad hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. The primary goal of the routing protocol is to obtain correct and efficient route establishment between a pair of source and destination nodes so that messages may be delivered in a timely manner. The general performance measures are the delay and throughput of information [4]. Due to the limited bandwidth associated with most wireless channels, it is obvious that route construction should be done with a minimum of overhead and bandwidth consumption. And due to the nature of node distribution, another performance measure is path reliability, which distinguishes ad hoc networks from other types of networks. Much work has appeared in these areas, but advances in wireless research are focusing more and more on the adaptation capability of routing protocols due to the interrelationship among these performance measures.

Routing algorithms, it is well known, determine the optimum path between *n* senders and receivers based on specific metrics, such as shortest time delay or minimum cost. Determination of optimal paths in large networks has been an area of active research for many years, with applications for travelling salesman, school bus routing, flight routings and others. An important factor in routing algorithm design is the time *T* it takes to develop a solution. If *T* is more than the average time between topology changes, then the algorithm cannot update the routing table fast enough. For example, if the topology changes every 20 seconds, but it takes a minute to find a route, then the routing tables will not have correct routing information and the whole routing system will collapse. This is the main challenge in MANET routing. In MANET, the internal routing algorithms do not work well because they assume that the topology will change very infrequently, thus an optimal path can be found almost at leisure [4].

For mobile ad hoc networks, the core routing functionalities include:

- Path generation to generate possible paths between the senders and receivers.
- Path selection to determine the appropriate paths based on a selection criteria (minimal time).
- Data forwarding to transmit user traffic along the selected paths.
- Path maintenance to make sure that the selected route is maintained and to find alternates in case of problems.
- Due to the nature of MANETs, the routing protocols should be highly adaptive, fast, and energy/bandwidth efficient.

B. *MANET Routing Algorithms*

Many routing protocols for MANET have been published. Although there are different ways of classifying them, a convenient approach is to view them in terms of small or large networks [6].

For smaller networks, the following are well known:

Dynamic Source Routing (DSR) uses a source (versus hop-by-hop) algorithm. Thus there is no need for intermediate nodes to maintain routing information.

Ad Hoc On-Demand Distance Vector (AODV) combines DSR with sequence numbering and other features to make it more efficient

In recent years, research efforts have been focusing on improving the performance of routing protocols in MANET. The MANET working group coordinates the development of several candidates among the protocols including OLSR and AODV. These protocols are classified into four classes based on the time when routing information is updated, the Proactive Routing Protocol (PRP), Reactive Routing Protocols (RRP), Hybrid Routing Protocol (HRP) and the Geographical Routing Protocol (GRP) [4], [6].

There are other classifications of routing protocols such as the distance vector (DV) class and link state (LS) class based on the content of the routing table. The DV protocols broadcast a list (vector) of distances to the destinations and each node maintains the routing table of the shortest paths to each known destination. On the other hand, the LS protocols maintain the topology of the network (links state). Each entry in LS routing table represents a known link. In LS routing, each node needs to calculate the routing table based on the local (links state) information in order to obtain a route to destination. Normally, the link state protocols are more stable and robust but much more complex than distance vector protocols. There are also instances of the above two family In MANET. The OLSR is the most widely used link state protocol, while AODV is the most popular distance vector protocol. We provide a general analysis of link state routing and distance vector routing in MANET respectively.

Another classification of routing protocols is source routing and hop-by-hop routing. In source routing, the source computes the complete path towards the destination, which consequently leads to loop-free routing. In hop-by-hop routing, each intermediate node computes the next hop itself. The nature of hop-by-hop routing reduces the chance of failed route in MANET, which suffers much faster topology changes than wired networks. Consequently, the source routing protocol in MANET, DSR, allows the intermediate nodes and even overhearing nodes to modify the route in order to adapt to the nature of MANET. Most MANET routing protocols such as OLSR and AODV have the hop-by-hop nature.

C. *Proactive Routing Protocols (PRP)*

In proactive (table-driven) protocols, nodes periodically search for routing information within a network. The control overhead of these protocols is foreseeable, because it is independent to the traffic profiles and has a fixed upper bound. This is a general advantage of proactive routing protocols.

DSDV: The Destination-Sequenced Distance-Vector (DSDV) Routing protocol is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements such as making it loop-free. The basic improvements made include freedom from loops in routing tables, more dynamic and less convergence time. Every node in the MANET maintains a routing table which contains list of all known destination nodes within the network along with number of hops required to reach to particular node [4], [7]. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers are used to identify stale routes thus avoiding formation of loops. To maintain consistency in routing table data in a continuously varying topology, routing table updates are broadcasted to neighbor's periodically or when significant new information is available. In addition to its time difference between arrival of first and arrival of the best route to a destination is also stored so that advertising of routes, which are likely to change soon, can be delayed. Thus avoiding the advertisement of routes, which are not stabilized yet, so as to avoid rebroadcast of route entries that arrive with node is supposed to keep the track of settling time for each route so that fluctuations can be damped by delaying advertisement of new route to already known and reachable destination thus reducing traffic. Fluctuating routes occurs as a node may always receive two routes to a destination with same sequence number but one with better metric later. But new routes received which take to a previously unreachable node must be advertised soon. Mobiles also keep track of the settling time of routes, or the weighted average time that routes to a destination will fluctuate before the route with the best metric is received. By delaying the broadcast of a routing update by the length of the settling time, mobiles can reduce network traffic and optimize routes by eliminating those broadcasts that would occur if a better route was discovered in the very near future. Consequently, the proactive routing protocols prefer link state routing because additional route calculation of link state routing doesn't contribute to delay.

OLSR: Optimized Link State Routing (OLSR) is a proactive, link state routing protocol specially designed for ad hoc networks. OLSR maintains Multipoint Relays (MPRs), which minimizes the control flooding by only declaring the links of neighbors within its MPRs instead of all links [4], [7]. The multicast nature of OLSR route discovery procedure can be integrated with the mobile IP management by embedding the mobile-IP agent advertisement into the OLSR MPR-flooding. This is important for the 4G global ubiquitous networks, which requires the wireless access network to be fully adhoc. Several extensions of OLSR are available that correspond to different network scenario. For fast changing MANET, provides a fast-OLSR version which reacts faster to topology changes than standard OLSR by enabling the fast moving nodes to quickly discover its neighbors and select a subset of their MPRs to establish connection to other nodes.

D. Reactive Routing Protocol (RRP)

The reactive (on-demand) routing protocols represent the true nature of ad hoc network, which is much more dynamic than infrastructure networks. Instead of periodically updating the routing information, the reactive routing protocols update routing information when a routing requirement is presented, consequently reducing the control overhead, especially in high mobility networks where the periodical update will lead to significant useless overhead.

AODV: Ad hoc On-demand Distance Vector Routing (AODV) is an improvement of the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. The on-demand routing protocols suffer more from frequent broken source-to-destination links than table driven routing due to the delay caused by on-demand route recalculation. AODV avoids such additional delay by using distance vector routing. There are some improved versions of AODV. A "source route accumulation" version of AODV which modifies the Routing REQuest (RREQ) and Routing REPly (RREP) messages in order to speed up the convergence of route discovery [4]. In order to reduce control overhead, a controlled flooding (CF) mechanism to reduce overlapped flooding messages for AODV is used.

The AODV algorithm is an improvement of DSDV protocol described above. It reduces number of broadcast by creating routes on demand basis, as against DSDV that maintains mutes to each known destination. When source requires sending data to a destination and if route to that destination is not known then it initiates route discovery. AODV allows nodes to respond to link breakages and changes in network topology in a timely manner. Routes, which are not in use for long time, are deleted from the table. Also AODV uses Destination Sequence Numbers to avoid loop formation and Count to Infinity Problem. An important feature of AODV is the maintenance of timer based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently [4], [7]. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves.

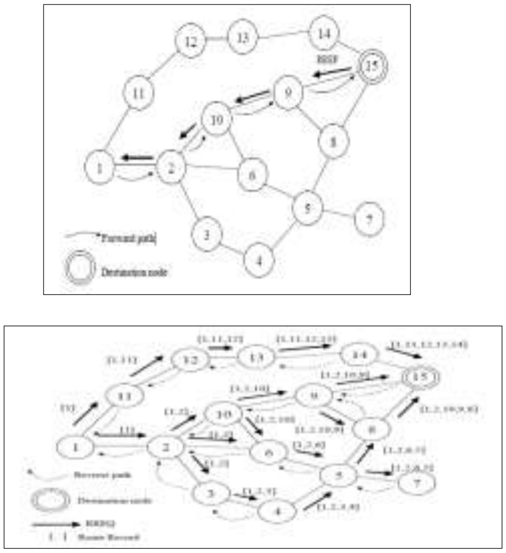

Figure 2. AODV routing protocol

DSR: The key feature of DSR is the use of source routing, which means the sender knows the complete hop-by-hop route to the destination. The node maintains route caches containing the source routes that it is aware of. Each node updates entries in the route cache as and when it learns about new routes [4], [6]. The data packets carry the source route in the packet headers. The delay and throughput penalties of DSR are mainly attributed to aggressive use of caching and lack of any mechanism to detect expired stale routes or to determine the freshness of routes when multiple choices are available. Aggressive caching, however, helps DSR at low loads and also keeps its routing load down.

The DSR is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of “Route Discovery” and “Route Maintenance’, which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on DSR protocol include easily guaranteed loop-free routing, operation in networks containing unidirectional links, use of only “soft state” in routing, and very rapid recovery when routes in the network change. In DSR, Route Discovery and Route Maintenance each operate entirely “on demand” [4], [7]. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any layer within the network.

The sender of a packet selects and controls the route used for its own packets, which together with support for multiple routes also allows features such as load balancing to be defined. In addition, all routes used are easily guaranteed to be loop-free, since the sender can avoid duplicate hops in the routes selected. The operation of both Route Discovery and Route Maintenance in DSR are designed to allow unidirectional links and asymmetric routes.

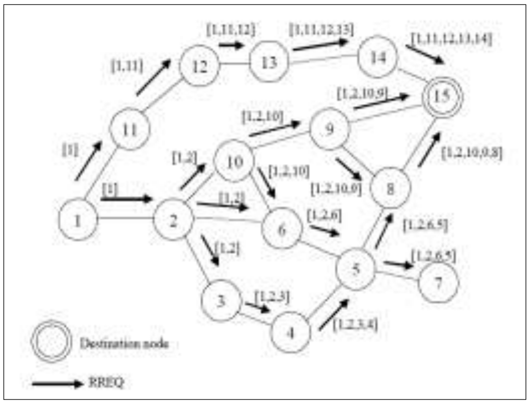

Figure 3. DSR Routing protocol

E. *Hybrid Routing Protocol*

The Ad Hoc network can use the hybrid routing protocols that have the advantage of both proactive and reactive routing protocols to balance the delay and control overhead (in terms of control packages). Hybrid routing protocols try to maximize the benefit of proactive routing and reactive routing by utilizing proactive routing in small networks (in order to reduce delay), and reactive routing in large-scale networks (in order to reduce control overhead) [4]. In the literature survey, hybrid routing protocols are compared with proactive routing protocol OLSR. The results show the hybrid routing protocols can achieve the same performance as the OLSR and are simpler to maintain due to its scalable feature. The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption.

ZRP: The Zone Routing Protocol (ZRP) localizes the nodes into sub-networks (zones). Within each zone, proactive routing is adapted to speed up communication among neighbors. The inter-zone communication uses on-demand routing to reduce unnecessary communication [4], [7]. An improved mathematic model of topology management to organize the network as a forest, in which each tree is a zone, was introduced. This algorithm guarantees overlap-free zones. Furthermore, the concept introduced in this algorithm also works with QoS control because the topology model is also an approach to estimate the link quality. An important issue of zone routing is to determine the size of the zone. An enhanced zone routing protocol, is the Independent Zone Routing (IZR), which allows adaptive and distributed reconfiguration of the optimized size of zone. Furthermore, the adaptive nature of the IZR enhances the scalability of the ad hoc network.

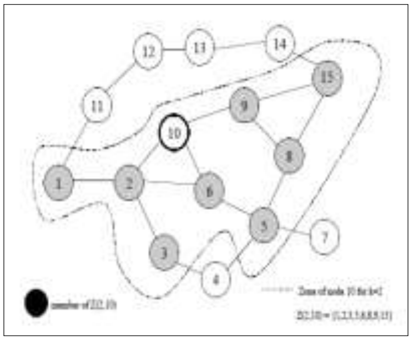

Figure 4. Zone Routing protocol

F. *Geographical Routing*

LAR: Location-Aided Routing (LAR) protocol is an approach that decreases overhead of route discovery by utilizing location information of mobile hosts. Such location information may be obtained using the global positioning system (GPS). LAR uses two flooding regions, the forwarded region and the expected region. LAR protocol uses location information to reduce the search space for a desired route, limiting the search space results in fewer route discovery messages. When a source node wants to send data packets to a destination, the source node first should get the position of the destination mobile node by contacting a location service which is responsible of mobile node positions. This causes a connection and tracking problems. Two different LAR algorithms have been presented. LAR scheme 1 and LAR scheme 2 [5]. LAR scheme 1 uses expected location of the destination (so-called expected zone) at the time of route discovery in order to determine the request zone. The request zone used in LAR scheme 1 is the smallest rectangle including current location of the source and the expected zone for the destination. The sides of the rectangular request zone are parallel to the X and Y axes. When a source needs a route discovery phase for a destination, it includes the four corners of the request zone with the route request message transmitted. Any intermediate nodes receiving the route request then make a decision whether to forward it or not, by using this explicitly specified request zone. Note that the request zone in the basic LAR scheme 1 is not modified by any intermediate nodes. On the other hand, LAR scheme 2 uses distance from the previous location of the destination as a parameter for defining the request zone. Thus, any intermediate node *j* receiving the route request forwards it if *j* is closer to or not much farther from the destination's previous location than node *i* transmitting the request packet to *j*. Therefore the implicit request zone of LAR scheme 2 becomes adapted as the route request packet is propagated to various nodes [8].

III. CHARACTERISTICS OF MANET

Mobile Adhoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust.

It does not require fixed infrastructure components such as access points or base stations. In a MANET, two or more devices are equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their radio range (peer-to-peer communication) or one that is outside their radio range by using intermediate nodes to relay the packets from the source to destination [4].

It causes route changes, sources may need to traverse multiple and different links to reach the destination every time because all nodes may be moving. Due to this, the traditional routing protocols fail because they assume fixed network topology.

It is self-organizing and adaptive. This means that a formed network can be formed on-the-fly without the need for any system administration. This allows rapid deployment of networks when needed and a quick teardown when not needed

It can consist of heterogeneous devices: i.e., the nodes can be of different types (PDAs, laptops, mobile phones, routers, printers etc) with different computation, storage and communication capabilities. The only requirement is that the basic MANET software has to be able to run in the devices.

Power consumption can be high because nodes have to be kept alive to forward data packets sent by other nodes that just happen to be in the neighborhood. This especially presents a challenge to the tiny sensors that participate in MANETs.

The characteristics of these networks are summarized as follows:

- Communication via wireless means.
- Nodes can perform the roles of both hosts and routers.
- No centralized controller and infrastructure. Intrinsic mutual trust.
- Dynamic network topology. Frequent routing updates.
- Autonomous, no infrastructure needed.
- Can be set up anywhere.
- Energy constraints
- Limited security

Generally, the communication terminals have a mobility nature which makes the topology of the distributed networks time varying. The dynamical nature of the network topology increases the challenges of the design of ad hoc networks. Each radio terminal is usually powered by energy limited power source (as rechargeable batteries). The power consumption of each radio terminal could be divided generally into three parts, power consumption for data processing inside the RT, power consumption to transmit its own information to the destination, and finally the power consumption when the RT is used as a router, i.e. forwarding the information to another RT in the network [9]. The energy consumption is a critical issue in the design of the ad hoc networks. The mobile devices usually have limited storage and low computational capabilities. They heavily depend on other hosts and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad Hoc networks.

A. *Network Security*

Network security extends computer security, thus all the things in computer security are still valid, but there are other things to consider as well. Network security is then computer security plus secure communication between the computers or other devices. Not all nodes are computers in an Ad Hoc network, thus nodes cannot be assumed to implement the security services normally existent in computers' operating systems. That is why network security should be defined as - Making sure that the nodes enforce a proper computer security and then securing the communication between them-. Different variables have different impact on security issues and design [4]. Especially environment, origin, range, quality of service and security criticality are variables that affect the security in the network. If the environment is concerned, networks can operate in hostile or friendly environments. A battlefield has totally different requirements for security if compared with home networks. On a battlefield also physical security and durability might be needed to ensure the functionality of the network.

The ways to implement security vary if the range of the network varies. If the nodes are very far from each other, the risk of security attacks increases. On the other hand, if the nodes are so close to each other that they actually can have a physical contact, some secret information (e.g. secret keys) can be transmitted between the nodes without sending them on air. That would increase the level of security, because the physical communication lines are more secure than wireless communication lines. Quality of service issues deal with questions like -Is it crucial that all messages reach their destination?- or -Is it crucial that some information reaches the destination in certain time?-. QoS is generally demanded in real time applications where reliable and deterministic communication is required. These issues refer to security e.g. in process control applications. We could have an Ad Hoc network in some process and all the measurements and control signals could be transmitted through the network. In order to have secure and reliable control of the process, quality of service requirements need to be met [4].

The last variable of Ad Hoc networks described with respect to security is security criticality. This means that before we think of the ways to implement security, we must consider carefully whether security is required at all or whether it matters or not if someone outside can see what packets are sent and what they contain. Is the network threatened if false packets are inserted and old packets are retransmitted? Security issues are not always critical, but it might cost a lot to ensure it. Sometimes there is trade-off between security and costs.

B. Security Problems in MANETs

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons:

- Open Medium - Eavesdropping is easier than in wired network.
- Dynamically Changing Network Topology - Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.
- Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
- Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system.
- Lack of Clear Line of Defense - The only use of first line of defense - attack prevention may not succeed. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link. In addition to prevention, we need second line of defense - detection and response.

Advantages

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.
- These networks work without any pre-existing infrastructure.

Disadvantages

Some of the disadvantages of MANETs are:

- Limited resources. Limited physical security.
- Intrinsic mutual trust vulnerable to attacks. Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

IV. Proposed Approach

We will evaluate the performance of our algorithm using ns-2 simulation [8]. Our institution has extended ns-2 with some wireless supports, including new elements at the physical, link, and routing layers of the simulation environment. Using these elements, it is possible to construct detailed and accurate simulations of ad hoc networks. For scenario creation, two kinds of scenario files are used to specify the wireless environment. The first is a movement pattern file that describes the movement that all nodes should undergo during the simulation. The second is a communication pattern file that describes the packet workload that is offered to the network layer during the simulation. To obtain the performance of MSR at different moving speeds, we will use two simulation sets with speeds of 1 and 25 m/sec, respectively. Our simulations model a network of 50 mobile hosts placed randomly within a 1500 m × 300 m area, both with zero pause time. To evaluate the performance of MSR, we experimented with different application traffic, including CBR and file transfer protocol (FTP). CBR uses UDP as its transport protocol, and FTP uses TCP. The channel is assumed error free except for the presence of collision.

We chose the following metrics for our evaluation –

- Network size: presented as number of nodes;
- Connectivity: the average degree of a node, normally presented as neighbors;
- Mobility: the topology of the network, relative position and speed of the node;
- Link capacity: bandwidth, bit error rate (BER), etc.
- Queue size: The size of the IFQ (Interface Priority Queue) object at a node
- Packet delivery ratio: The ratio between the number of packets originated by the “application layer” CBR sources

and the number of packets received by the CBR sink at the final destination

- Data throughput: The total number of packets received during a measurement interval divided by the measurement interval
- End-to-end delay
- Packet drop probability
- Average Delay or end-to-end delay
- Hop count
- Message Delivery Ratio
- Normalized routing overload

It is necessary to fine tune the performance measures outlined above such that our proposed criteria has significant advantages over already developed techniques. We have described in great detail the performance measure of path reliability. Path generation to generate possible paths between the senders and receivers and path selection to determine the appropriate paths based on minimal time, will be highlighted in our research. Furthermore, our proposed technique will be highly adaptive, fast and energy/bandwidth efficient.

V. Conclusion

As this paper is a research in progress, there has not been a section for discussions laid out here. Nevertheless the issues and highlights about MANET in battlefield zones have been expressed in great detail. Ad hoc networks can be implemented using various techniques like Bluetooth or WLAN for example. The definition itself does not imply any restrictions to the implementing devices. Ad Hoc networks need very specialized security methods. There is no approach fitting all networks, because the nodes can be any devices. The computer security in the nodes depends on the type of node and no assumptions on security can be made. In this paper, the computer security issues have not been discussed, because the emphasis has been on network security.

But with the current MAC layer and routing solutions the true and working ad hoc network is just a dream for now. However, it can be used with relatively small networks and potentially some very nice applications can be realized. Although some peer-to-peer type of solutions work nicely already today, it would be nice to see that some new and innovative solutions would be seen in the arena of ad hoc networks since it is not hard for one to imagine a countless number of nice and ad hoc based applications.

Advances in ad hoc network research have opened the door to an assortment of promising military and commercial applications for ad hoc networks. However, because each application has unique characteristics, (such as traffic behavior, device capabilities, mobility patterns, operating environments, etc.) routing in such a versatile environment is a challenging task, and numerous protocols have been developed to address it. While many protocols excel for certain types of ad hoc networks, it is clear that a single basic protocol cannot perform well over the entire space of ad hoc networks. To conform to any arbitrary ad hoc network, the basic protocols designed for the edges of the ad hoc network design space need to be integrated into a tunable framework.

As such there has been a lot of research on routing protocols and their impact on network transmission rates and delay. These protocols have significant advantages in their own right and are best suitable for each circumstance in their mode or operating environment. There cannot be a single protocol that is judged as the best of its class and so we have made sure that each category of routing protocol is elaborately described and characterized.

In addition, more research has to be done regarding to network size, mobility, queue size and normalized routing overload parameters.We will continue our work into this regard in future publications and will attempt our best to discuss more about the physical, link and routing layers of the simulation environment.

VI. Future Research

The emphasis in this paper has been on garnering knowledge in the areas of wireless MANET and their applications in battlefield operations. We have made the best effort to keep abreast of technical developments in this area and so our efforts in documenting our research results and discussions have not been made. In phase II of our future research, we will deploy the settings and performance parameters as outlined in the text, to our research goals. Future scope will include simulating the network parameters such as network size, connectivity, bit error rate, bandwidth and queue size. Spatial location issues such as geolocation will be emphasized using geographical routing algorithms. Using the Global Positioning System (GPS), location aided routing will be used to reduce the search space in fewer route discovery messages. Also, in order to have secure and reliable control of the process, Quality of Service (QoS) requirements will be met.

References

[1]. N.H. Saeed, M.F. Abbod, H.S. Al-Raweshidy, "Modeling MANET Utilizing Artificial Intelligent," *Second UKSIM European Symposium on Computer Modeling and Simulation*, 2008, pp. 117-122.

[2]. Mobile Ad-hoc Networks (manet) Working Group (http://www.ietf.org/html.charters/manet-charter.html.

[3]. Mobile Computing and Wireless Communications by Amjad Umar, NGE Solutions, Inc. 2004.

[4]. The *Handbook of Ad Hoc Wireless Networks* by Mohammad Ilyas, CRC Press, 2003.

[5]. Routing protocols for mobile ad-hoc networks: Current development and evaluation by Zhijiang Chang, Georgi Gadadijev, Stamatis Vassiliadis, 2007.

[6]. Kniess, J; Loques, O; Alberquerque, C.V.N, “Location aware discovery services and selection protocol in cooperative mobile wireless ad hoc networks”, *IEEE Infocom workshop* 2009, pp. 1-2.

[7]. Ashtrani, H; Nikpour, M; Moradipour, H, “A comprehensive evaluation of routing protocols for ordinary and large-scale wireless MANETs”, *IEEE International conference on networking, architecture, and storage*, 2009, 167-170.

[8]. “Network Simulator,” http://www.isi.edu/nsnam/ns.

[9]. Mohammad A. Mikki, “Energy Efficient Location Aided Routing Protocol for wireless MANETs”, *in International Journal of Computer Science and Information Security, Vol 4,* No. 1&2, 2009.

AUTHORS PROFILE

Dr. C. Rajabhushanam is with the computer science engineering department at Tagore Engineering College, Rathinamangalam, Chennai, Tamilnadu 600048, India (e-mail: rajcheruk@gmail.com).

Dr. A. Kathirvel is with the computer science and engineering department at Tagore Engineering College, Rathinamangalam, Chennai, Tamilnadu 600048, India (e-mail:kathir.tagore@gmail.com).