THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Evaluation of Routing Protocols and Security Issues for MANET

Amit Pratap Singh
DIT College, UTU University, Dehradun, Uttrakhand, India
Er. Nitin Thapliyal
Assistant Proffessor, DIT College, UTU University, Dehradun, India

Abstract:
In this era of wireless devices, Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. This Paper presents a coherent survey on MANET – Mobile Ad Hoc Network, with the intent of serving as a quick reference to the current research in ad hoc networking. It starts with a background on the origin and deployment constraints of ad hoc network fully distinguishing it from traditional network. This paper discusses a broad range of research issue such as Routing Protocols and Security issues.

Ad hoc networks are characterized by multi-hop wireless connectivity, frequently changing network topology and the need for efficient dynamic routing protocols plays an important role. In this paper we compare the performance of three on-demand routing Protocols for mobile Ad-hoc network (MANET) networks: Dynamic Source Routing (DSR), Ad Hoc On-demand distance Vector Routing (AODV) and Temporarily Ordered Routing Algorithm (TORA) in by varying the size of the networks. The performance metrics selected to make the performance differences are Total Traffic Received, Traffic Load, Throughput, Number of Hops per Route and Route Discovery Time. AODV shows a Considerable better performance over the others for any number of nodes. TORA and DSR show moderate performance for minimum number of nodes, where in the case of large networks, DSR shows some performance rather than TORA.

Parallely it provides an overview of routing protocols by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. The wireless links in ad hoc network are highly error prone as it is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure, so it can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSR, AODV,DSDV and TORA. However the AODV and DSDV are perform very well when mobility is high. Security is a big issue in MANETs as they are infrastructure-less and autonomous. This paper will address some basic security concerns in MANET.

This paper would be a great help for the people conducting research on real world problems in MANET routing protocols as well as its security.

Key words: *Quality of Service, Security, ad hoc routing protocol, Countermeasures*

1. Introduction

Mobile ad-hoc network (MANET) routing protocols play a fundamental role in a possible future of ubiquitous devices. Current MANET commercial applications have mainly been for military applications or emergency situations. However, we believe that research into MANET routing protocols will lay the groundwork for future wireless sensor networks and wireless plug-n-play devices. The challenge is for MANET routing protocols to provide a communication platform that is solid, adaptive and dynamic in the face of widely uctuating wireless channel characteristics and node mobility.

A Mobile Ad hoc Network (MANET) is an autonomous system of nodes (MSs) connected by wireless links. It doesn't need support from any existing network infrastructure like an Internet gateway or other fixed stations.

MANET (Mobile ad hoc network) is a temporary self organizing system formed by a Collection of nodes, which are connected with wireless links. In the network, nodes may be disappeared or new nodes may be appeared over the time due to node mobility. In the recent years, many researchers are contributing to the improvement of the performance of routing protocols in MANET. IETF (Internet Engineering Task Force) created a working group in 1996 to deal with the MANET research. The idea of such networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. The network's wireless topology may dynamically change in an unpredictable manner since nodes are free to move and information is transmitted in a store-and forward manner using multi hop routing. 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.

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.

This paper will evaluate the performance of three on demand routing protocols for mobile Ad-hoc network (MANET): Dynamic Source Routing (DSR), Ad Hoc On demand distance Vector Routing (AODV) and Temporarily Ordered Routing Algorithm (TORA) by varying the size of the networks. The performance metrics selected to make the performance evaluations are Total Traffic Received, Traffic Load, Throughput, Number of Hops per Route and Route Discovery Time. This analysis was done using the MANET model in OPNET simulaton. OPNET Simulator is the industry's leading simulator specialized for network research and development. It allows to design and study communication networks, devices, protocols, and applications with great flexibility. This paper defines the mobile ad hoc routing protocols categories and the overview of AODV, DSR and TORA protocols. Finally, simulation environment and performance metrics and some possible countermeasures against the security attack are described.

In some application environment, such as battlefield communications, national crises, disaster recovery (fire, flood, earth quake) etc., the wired network is not available and ad hoc networks provide the only feasible means for communications and information access. Also Ad hoc network is now playing important role in civilian forums such as campus recreations, conferences, electronic classrooms etc. The vision of ad hoc networks is wireless Internet, where users can move anywhere anytime and still remaining connected with the rest the world.

2. Routing Protocols

A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes and numerous routing protocols have been proposed for such kind of ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols have been an active area of research for many years. Many protocols have been suggested keeping applications and type of network in view. Basically, routing protocols can be broadly classified into two types as (a) Table Driven Protocols or Proactive Protocols and (b) On-Demand Protocols or Reactive Protocols

- **Table Driven or Proactive Protocols:** In Table Driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some of the existing table driven or proactive protocols are: DSDV, DBF, GSR, WRP, and ZRP.
- **On Demand or Reactive Protocols:** In these protocols, routes are created as and when required. When a transmission occurs from source to destination, it invokes the route discovery procedure. The route remains valid till destination is achieved or until the route is no longer needed. Some of the existing on demand routing protocols are: DSR, AODV, and TORA. The emphasis in this research paper is concentrated on the survey and comparison of various On Demand/Reactive Protocols such as DSR, AODV and TORA as these are best suited for Ad Hoc Networks. The next sub-section describes the basic features of these protocols.

2.1. Desirable properties of Ad-Hoc Routing protocols

The properties that are desirable in Ad-Hoc Routing protocols are:

- **Distributed operation:** The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The difference is that the nodes in an ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.
- **Loop free:** To improve the overall performance, the routing protocol should guarantee that the routes supplied are loop free. This avoids any waste of bandwidth or CPU consumption.
- **Demand based operation:** To minimize the control overhead in the network and thus not waste the network resources the protocol should be reactive. This means that the protocol should react only when needed and that the protocol should not periodically broadcast control information.
- **Unidirectional link support:** The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.
- **Security:** The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network.
- **Power conservation:** The nodes in the ad-hoc network can be laptops and thin clients such as PDA's that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.
- **Multiple routes:** To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.
- **Quality of Service Support:** Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for. It could be for instance real time traffic support. It should be noted that none of the proposed protocols have all these properties, but it is necessary to remember that the protocols are still under development and are probably extended with more functionality.

3. Ad-Hoc on Demand Distance Vector

AODV is a variation of Destination-Sequenced Distance-Vector (DSDV) routing protocol which is collectively based on DSDV and DSR. It aims to minimize the requirement of system-wide broadcasts to its extreme. It does not maintain routes from every node to every other node in the network rather they are discovered as and when needed & are maintained only as long as they are required. It is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. It is a modification of DSDV. The demand on available bandwidth is significantly less than other proactive protocols as AODV doesn't require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes. AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV. Sequence numbers serve as time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path. The key steps of algorithm used by AODV for establishment of unicast routes are Route Discovery, Expanding Ring Search Technique, Setting up of Forward Path, Route Maintenance

3.1. Looking at working of AODV

We take an example of five mobile nodes as shown in Figure 3.1. The circles indicate the range of communication for the nodes. As each node has a limited communication range, it can communicate with its neighbor nodes only. At an instant, Node 4 wants to communicate with Node 3, but it is uncertain of the route. Node 4 broadcasts RREQ that is received by its neighbors Node 1 and Node 5. Node 5 doesn't have any route to Node 3 and therefore it rebroadcasts RREQ that is received back by Node 4. Node 4 drops it. On the other side, if Node 1 has a greater sequence number than RREQ, it discards RREQ and replies with RREP. If not, it updates the sequence number in its routing table and forwards RREQ to Node 2. As Node 2 has a route to Node 3, it replies to Node 1 by sending an RREP. Node 1 sends RREP to Node 4 and route Node 4-Node 1-Node 2-Node 3 is confirmed to send data packets. Node 4 can now send data packets to Node 3 through the specified route. Imagine a Node 6 in the communication range of Node 1 and Node 2. As shown in Figure3.2, Node 1 moves out of network. Suppose Node 6 detects it first by not getting any HELLO message from Node 1and marks the respective route table entry for route as invalid. It sends out an RERR with the invalid route which is received by Node 2. This is how Node 2 comes to know from Node 6 that Node 1 is no longer its neighbor.

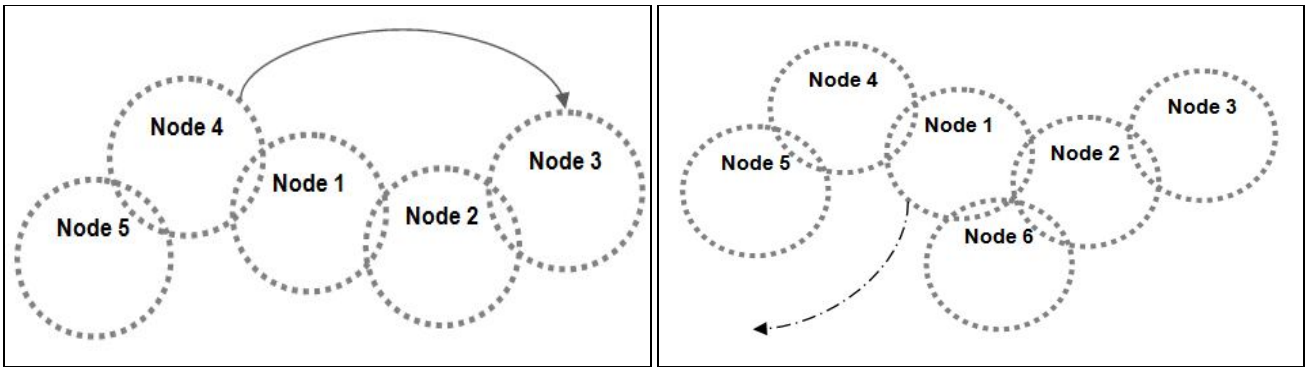

Figure 3.1: Communication between nodes in a Mobile Ad-hoc Network
Figure 3.2: Node 1 moves out of communication range

3.2. Security Attacks against AODV

As MANETs are unwired network with dynamic topology associated with them, they are very vulnerable to MANET attacks. In protocol stack, Physical layer has security issues like Denial of Service (DoS) attacks and preventing signal jamming. Network layer has to deal with security of ad-hoc routing protocol and related parameters. Transport layer has issues with end to end data security with encryption methods and Authentication. Application layer has security concerns with prevention, worms, malicious codes, application abuses as well as virus detection.

There can be two kinds of attacks: passive and active. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for MANET.

3.2.1. Attacks using Modification

A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, AODV uses the hop count parameter. A malicious node can set the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A DoS attack may be launched by modifying source routes as well. DoS attack is easy to carry out but it is difficult to detect.

3.2.2. Attacks using Impersonation

By impersonating a node (spoofing), a malicious node can cause lots of attacks in MANET. For example, traffic that belongs to the impersonated node may be redirected to the malicious node. Loops may also be created by spoofing. The malicious node may take up identity of multiple nodes; it does not need to impersonate any node of the network.

3.2.3. Attacks using Fabrication

In fabrication attacks, false routing information is generated by an intruder. For example, false route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known fabrication attacks are described here:

1.Blackhole attacks, 2. Grayhole attacks, 3. Wormhole attacks.

3.3. Securing AODV

To make AODV secure, we need to understand security attributes and mechanisms. Security is applied with the mixture of processes, procedures, and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation.

As MANETs use an open medium, all nodes can access data within the communication range. Therefore, confidentiality should be obtained by preventing the unauthorized nodes to access data. Authentication should be used to ensure the identity of source as well as neighbor nodes to prevent a node from accessing unauthorized resources and confidential information as well as to stop it from interfering operations of other nodes. Integrity helps to prevent malicious nodes from altering data and resending it (called replay attack e.g. wormhole attack). Also, if a node sends a message, that node cannot deny that the message was sent by it which is called non repudiation.

To defend against passive attacks conventional approaches like digital signature, encryption, authentication and access control (whether a node having appropriate access rights to access the network) should be considered. To defend against active attacks intrusion detection systems and cooperation enforcement mechanisms (reducing selfish behavior of a node) are useful. Encryption and authentication are based on asymmetric and symmetric cryptography. To achieve data integrity and authentication, hash functions and digital signatures are really useful.

Secure Ad-hoc On Demand Distance Vector (SAODV) is an extension of AODV in which digital signature and has chains mechanisms are used. Every node uses digital signature for authentication and integrity in routing messages like RREQ, RREP and RRER. This signature is verified by neighbor nodes that receive the message. Hash chains are used to secure hop-count mechanism. Thus, SAODV addresses security of routing messages only; security of data exchange still remains unaddressed. Moreover, due to digital signatures, messages get bigger. Also, generating and verifying signatures add to the overhead, especially when double signatures mechanism is used.

3.4. Benefits and Limitations of AODV

The benefits of AODV protocol are that it favors the least congested route instead of the shortest route and it also supports both unicast and multicast packet transmissions even for nodes in constant movement. It also responds very quickly to the topological changes that affects the active routes. AODV does not put any additional overheads on data packets as it does not make use of source routing. The limitation of AODV protocol is that it expects/requires that the nodes in the broadcast medium can detect each others' broadcasts. It is also possible that a valid route is expired and the determination of a reasonable expiry time is difficult. The reason behind this is that the nodes are mobile and their sending rates may differ widely and can change dynamically from node to node. In addition, as the size of network grows, various performance metrics begin decreasing. AODV is vulnerable to various kinds of attacks as it based on the assumption that all nodes must cooperate and without their cooperation no route can be established.

4. Dynamic Source Routing

Dynamic Source Routing (DSR) is a reactive kind of protocol which reacts on-demand. The main feature of DSR is source routing in which the source always knows the complete route from source to destination. It frequently uses source routing and route caching. Route Discovery and Route Maintenance are two main methods used in DSR. It is uncomplicated and efficient protocol. It does not depend on timer-based activities. It allows multiple routes to destination node and routing is loop-free here. Any broken link is notified to the source node with an error message. It works well in large networks where routes change quickly and mobility of routes is higher. In DSR, intermediate nodes do not need to preserve the routing information. Instead the packets themselves contain every routing decision. DSR uses a route discovery process to find a route when a node in the network tries to send a data packet to a destination for which the route is unknown. A route is found by flooding the network with route requests. When a node receives this request, it broadcasts it again until it itself is the destination or it has the route to the destination. This node then replies to the request to the original source. The request and response packets are source routed. Request packet creates the path of traversal. Response packet creates the reverse path to the source by traversing backwards.

DSR is an Ad Hoc routing protocol which is based on the theory of source-based routing rather than table-based. This protocol is source-initiated rather than hop-by-hop. This is particularly designed for use in multi hop wireless ad hoc networks of mobile nodes. Basically, DSR protocol does not need any existing network infrastructure or administration and this allows the Network to be completely self organizing and self-configuring. This Protocol is composed of two essential parts of route discovery and route maintenance. Every node maintains a cache to store recently discovered paths. When a node desires to send a packet to some node, it first checks its entry in the cache. If it is there, then it uses that path to transmit the packet and also attach its source address on the packet. If it is not there in the cache or the entry in cache is expired (because of long time idle), the sender

broadcasts a route request packet to all of its neighbors asking for a path to the destination. The sender will be waiting till the route is discovered. During waiting time, the sender can perform other tasks such as sending/forwarding other packets. As the route request packet arrives to any of the nodes, they check from their neighbor or from their caches whether the destination asked is known or unknown. If route information is known, they send back a route reply packet to the destination otherwise they broadcast the same route request packet. When the route is discovered, the required packets will be transmitted by the sender on the discovered route. Also an entry in the cache will be inserted for the future use. The node will also maintain the age information of the entry so as to know whether the cache is fresh or not. When a data packet is received by any intermediate node, it first checks whether the packet is meant for itself or not. If it is meant for itself (i.e. the intermediate node is the destination), the packet is received otherwise the same will be forwarded using the path attached on the data packet. Since in Ad hoc network, any link might fail anytime. Therefore, route maintenance process will constantly monitors and will also notify the nodes if there is any failure in the path. Consequently, the nodes will change the entries of their route cache.

4.1. Benefits and Limitations of DSR

One of the main benefit of DSR protocol is that there is no need to keep routing table so as to route a given data packet as the entire route is contained in the packet header. The limitations of DSR protocol is that this is not scalable to large networks and even requires significantly more processing resources than most other protocols. Basically, In order to obtain the routing information, each node must spend lot of time to process any control data it receives, even if it is not the intended recipient.

5. TORA (Temporary Ordered Routing Protocol)

Temporally-Ordered Routing Algorithm (TORA) is made to find routes on demand. It tries to achieve high scalability. It creates and maintains directed acyclic graph rooted at the destination node. TORA can establish routes rapidly and can provide multiple routes for a single destination. It doesn‟t give Shortest-Path Algorithm too much of importance. Instead it uses longer paths to avoid finding of new routes. TORA minimizes communication over as it reacts only when needed and doesn‟t react to every topological change as well as it localizes scope of failure reactions.

There are three main phases of the algorithm: Route Creation, Route Maintenance and Route Erasure. In the Route Creation phase, the query packet is flooded all over the network and if routes exist, an update packet is sent back. In the Route Maintenance phase update packets re-orient the route composition. The route erasure phase involves flooding of a broadcast clear packet all over the network to erase invalid routes. To simulate the protocol, size of network, rate of topological change and network connectivity should be kept in mind.

TORA is a distributed highly adaptive routing protocol designed to operate in a dynamic multihop network. TORA uses an arbitrary height parameter to determine the direction of link between any two nodes for a given destination. Consequently, multiple routes often exist for a given destination but none of them are necessarily the shortest route. To initiate a route, the node broadcasts a QUERY packet to its neighbors. This QUERY is rebroadcasted through the network until it reaches the destination or an intermediate node that has a route to the destination. The recipient of the QUERY packet then broadcasts the UPDATE packet which lists its height with respect to the destination. When this packet propagates in the network, each node that receives the UPDATE packet sets its height to a value greater than the height of the neighbour from which the UPDATE was received. This has the effect of creating a series of directed links from the original sender of the QUERY packet to the node that initially generated the UPDATE packet. When it was discovered by a node that the route to a destination is no longer valid, it will adjust its height so that it will be a local maximum with respect to its neighbours and then transmits an UPDATE packet. If the node has no neighbors of finite height with respect to the destination, then the node will attempt to discover a new route as described above. When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad hoc network.

5.1. Benefits and Limitations of TORA

One of the benefits of TORA is that the multiple routes between any source destination pair are supported by this protocol. Therefore, failure or removal of any of the nodes is quickly resolved without source intervention by switching to an alternate route. TORA is also not free from limitations. One of them is that it depends on synchronized clocks among nodes in the ad hoc network. The dependence of this protocol on intermediate lower layers for certain functionality presumes that the link status sensing, neighbor discovery, in order packet delivery and address resolution are all readily available. The solution is to run the Internet MANET Encapsulation Protocol at the layer immediately below TORA. This will make the overhead for this protocol difficult to separate from that imposed by the lower layer.

5.2. Performance Metrics

There are number of qualitative and quantitative metrics that can be used to compare reactive routing protocols. Most of the existing routing protocols ensure the qualitative metrics. Therefore, the following different quantitative metrics have been considered to make the comparative study of these routing protocols through simulation.

- **Routing overhead:** This metric describes how many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.
- **Average Delay:** This metric represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It is measured in seconds.
- **Throughput:** This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps. It can also be defined as the total amount of data a receiver actually receives from sender divided by the time taken by the receiver to obtain the last packet.

- **Media Access Delay:** The time a node takes to access media for starting the packet transmission is called as media access delay. The delay is recorded for each packet when it is sent to the physical layer for the first time.
- **Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets.
- **Path optimality:** This metric can be defined as the difference between the path actually taken and the best possible path for a packet to reach its destination.

6. Simulation Environment

It is very difficult to estimate the performance of a proposed network in real life and as a result, many network simulators have been proposed to design and simulate networks in many perspectives. In the paper, simulation is performed on OPNET simulator. In the simulation, a 500 x 500 meters square geographical area is selected with varying number of MANET workstations where 30% of the total nodes are source-destination pairs. One third of the total nodes in any scenario are mobile nodes, moving according to Random Waypoint Mobility Model. A predefined trajectory "manet_down_left" is used in every network. Each mobile node waits for 260 seconds and starts moving along the path defined in the trajectory. The rest of the nodes are stationary nodes. Many different networks of small size like 20, 50 nodes and large size like 150,200 nodes are made to make the different scenarios. Sources start traffic generations exponentially at 100 seconds and continue till the end of the simulations. The performance metrics selected to make the performance differences are:

- Total Traffic Received
- Traffic Load
- Throughput
- Route Discovery Time
- Number of Hops per Route

7. Simulation Results and Analysis

The simulation results are shown in the following section and comparison between the three protocols are performed by varying numbers of nodes on the basis of the abovementioned metrics.

7.1. Total Traffic Received

Based on MANET Traffic Received between the protocols for different network sizes, the following figures show packets received per second. For 20 nodes, after 8-10 minutes, the figure 7.1 shows, AODV and DSR receiving almost the same number of packets where TORA receiving almost the half of them. The packet receiving performance of AODV and DSR increases exponentially as increasing the number of nodes. For 150 nodes, the figure 7.2 show,the performance curves for DSR is downward after 5 minutes simulation but for AODV, the curve is upward.

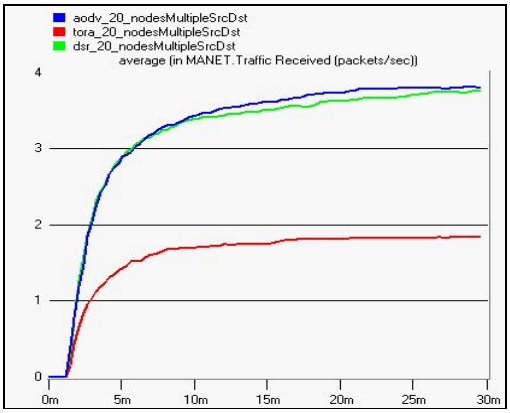

Figure 7.1: Total Traffic Received for 20 nodes

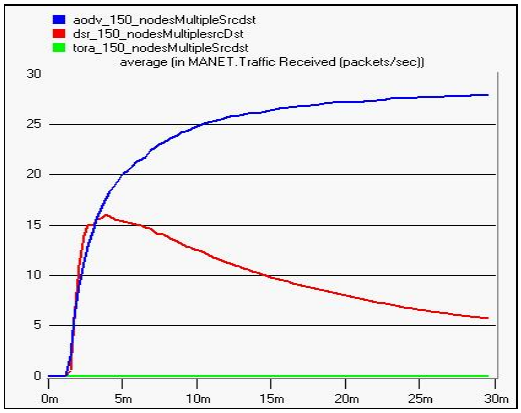

Figure 7.2: Total Traffic Received for 150 nodes

7.2 Traffic Load and Throughput

Based on Wireless LAN Load and Throughput, the following figures show that, for different number of nodes, loads are varying compared to each other. For 150 nodes, load for DSR network increased alarmingly. For any load, AODV is showing a considerable good performance.

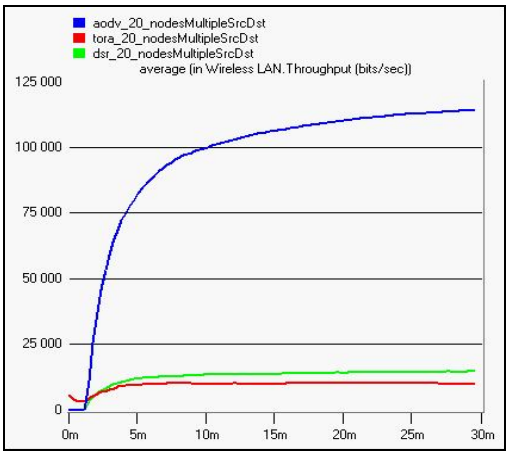

Figure 7.3: Wireless LAN load for 20 nodes

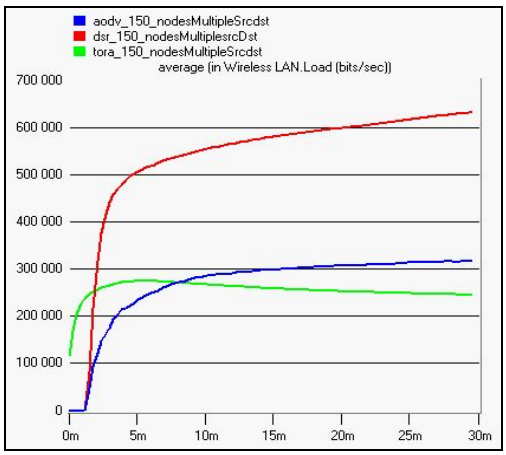

Figure 7.4: Wireless LAN load for 150 nodes

For a small network such as 20 nodes network, AODV has a good throughput compared to DSR and TORA. For a large network such as 150 nodes or 200 nodes, TORA has a minimum throughput where AODV is performing well.

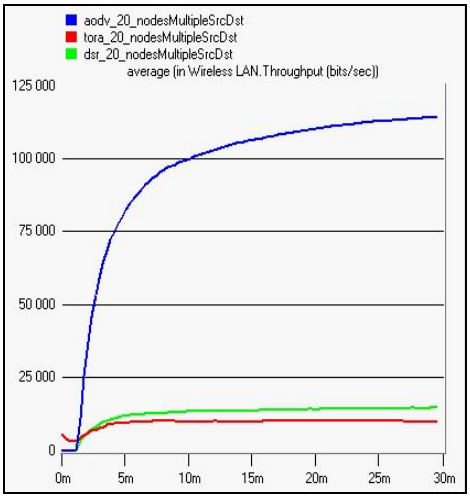

Figure 7.5: Wireless LAN Throughput for 20 nodes

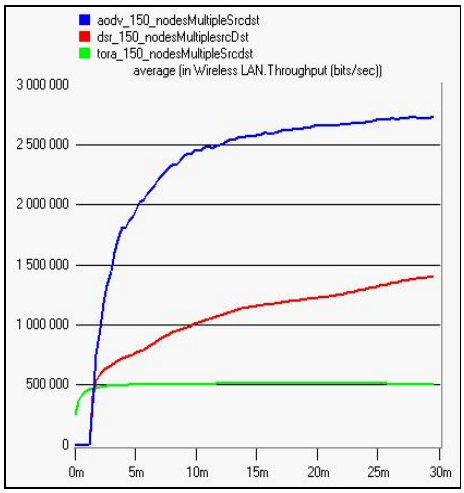

Figure 7.6: Wireless LAN Throughput for 150 nodes

7.3. Route Discovery Time and Number of Hops between AODV and DSR

Based on number of hops required and route discovery time between AODV and DSR, the following figures show that for any number of nodes, AODV performing better than DSR. For 150 nodes, route discovery time ranging from 2.5 seconds to 3.8 seconds for DSR throughout the simulation and that's why DSR needs more hops than AODV in every route. AODV has an excellent performance, taking less route discovery time and less number of hops per route.

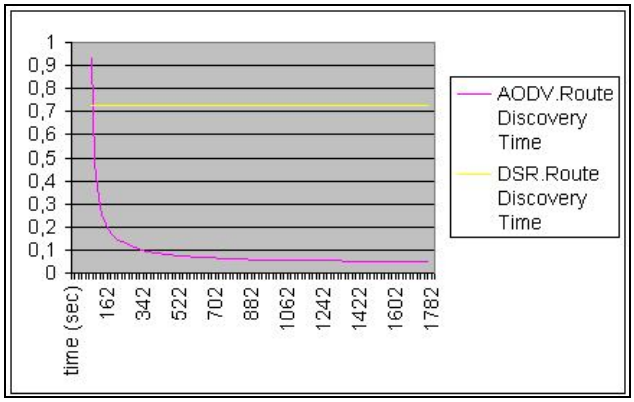

Figure 7.7: Route Discovery Time for 50 nodes

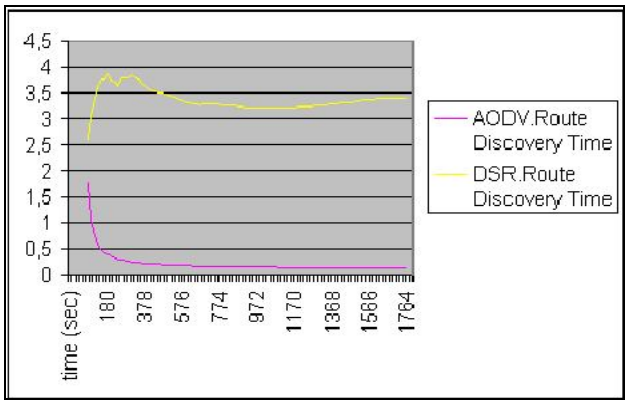

Figure 7.8: Route Discovery Time for 150 nodes

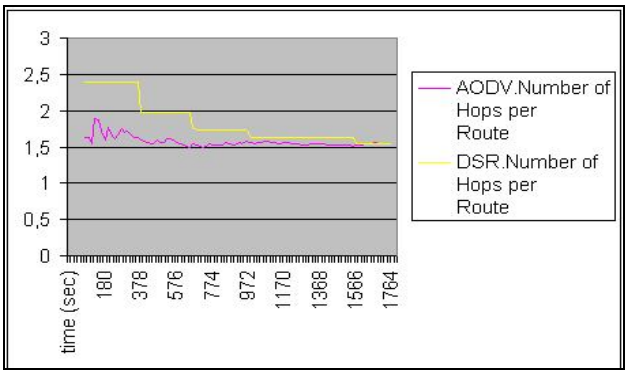

Figure 7.9: Number of Hops for 50 nodes

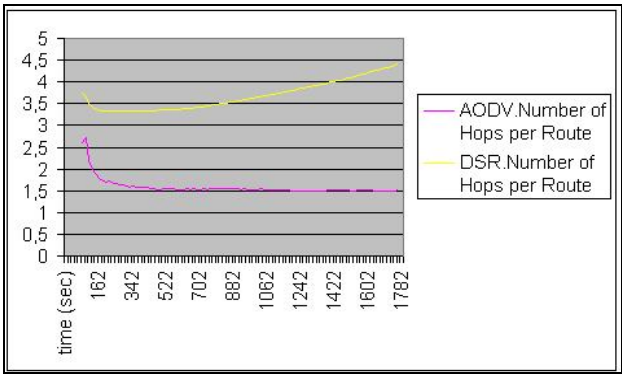

Figure 7.10: Number of Hops for 150 nodes

8. Security Issues

Performing communication in free space and the broadcast nature of ad hoc networks expose it to security attacks. Ad hoc wireless links are susceptible to attacks ranging from passive eavesdroping to active ipersonation, message replay and message distortion. Active attacks might allow the adversary to delete messages, inject errorneous, modify messages and impersonate a node , thereby voilating availability, integrity, authentication and nonrepudation.

Security is often considered to be the major ”roadblock” in commercial application of ad hoc network technology. In civilian, specially commercial, application even mere lack of cooperation may be enough to bring the network on its knees.

Understanding possible form of attacks is always the first step towards developing good security solution. Two types of security mechanism can generally be applied: Preventive and Detective. Preventive mechanism are typically based on key-based cryptography. However, designing secure key distribution that allows the creation of unforgeable credentials in ad hoc networks is a challenging problem. Diffie-Hellman key exchange may indeed help to establish some temporary security between particular end points. However, they are also vulnerable to the man-in-the-middle attacks.

The intrusion detection field studies how to discover that an intruder is attempting to penetrate the network to perform an attack. Most of the intrusion detection techniques developed on fixed wired network is not applicable to ad hoc network environment, as there are no traffic concentration points(Switches, Routers etc) where the intrusion detection system(IDS) can collect audit data for the entire network. The only available audit trace will be limited to communication activity taking place within the radio range and the intrusion detection algorithm must relay on this partial and localized information. A proposal for a new intrusion detection architecture that is both distributed and cooperative is presented in. Here all notes in the wireless ad hoc network participate in intrusion detection and reaction. Each node is responsible for detecting science of intrusion locally and independently, but neighbours can collaboratively investigate in a broader range. The Intrusion-resistant Ad Hoc Routing Algorithm(TIARA) is designed against denial of service attacks. The TIARA mechanism limit the damage caused by intrusion attacks and allow for continued network operation at an acceptable level during such attacks. The authenticated routing for ad hoc network (ARAN) protocol is an on demand , secure, routing protocol that detects and protects against malicious actions carried out by third parties in the ad hoc environment. The Secure Efficient Ad Hoc Distance (SEAD) is a proactive secure routing protocol based on DSDB. SEAD deals with attackers that modify a routing table update message. The basic idea is to authenticate the sequence number and the metric field of a routing table update message using one way hash function. Hash chains and digital are used by the SAODV mechanism to secure AODV.

Node cooperation enforcing is also an important issue i n providing a secure ad hoc network. A node that does not cooperate is called misbehaving node. Routing- Forwarding misbehaviours can be caudes by nodes that are malicious or selfish. A malicious node does not cooperate because it want to intentionally damage network functioning by dropping packets. On the other hand, a selfish node does not intent to directly damage other nodes, but is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf.

To cope with these problems a self-organising network must be based on an incentive for users to collaborate, thus avoiding selfish behavior.

9. Conclusion

In this research paper, an effort has been made to concentrate on the comparative study and performance analysis of various on demand/reactive routing protocols (DSR, AODV and TORA) on the basis of above mentioned performance metrics. TORA MANET models, which are the most commonly used models in Ad hoc routing. In the paper, the performance difference is made between three protocols for different number of nodes In the paper, detail analysis of the behavior of protocols based on some important metrics such as traffic sent and received, route discovery time and number of hops per route, load and throughput is performed. The network load is selected for small size like 20, 50nodes and large size 150, 200 nodes in which one third are mobile nodes and the rest of them are stationary nodes. Multiple sources and destinations are used in every scenario. AODV and DSR receive traffics for any number of nodes but TORA creates a lot of loads in large networks like 150, 200 nodes and cannot receive considerable traffics. As a result, AODV and DSR have better performance than TORA for maximum as well as minimum number of nodes. But above of all, AODV is showing the best performance over the others in every
respect. Only Random Waypoint Mobility Model is used in this paper due to the limitation of OPNET simulator. Therefore in future different mobility models with varying mobility of nodes should be measured along with different security issues.
The description of parameters selected with respect to low mobility and lower traffic. It has been observed that the performance of all protocols studied was almost stable in sparse medium with low traffic. TORA performs much better in packet delivery owing to selection of better routes using acyclic graph. Evaluation of same parameters with increasing speed and providing more nodes. The results indicate that AODV keeps on improving with denser mediums and at faster speeds. Description of other important parameters that make a protocol robust and steady in most cases. The evaluation predicts that in spite of slightly more overhead in some cases DSR and AODV outperforms TORA in all cases. AODV is still better in Route updating and maintenance process.
It has been further concluded that due to the dynamically changing topology and infrastructure less, decentralized characteristics, security and power awareness is hard to achieve in mobile ad hoc networks. Hence, security and power awareness mechanisms should be built-in features for all sorts of applications based on ad hoc network. The focus of the study is on these issues in our future research work and effort will be made to propose a solution for routing in Ad Hoc networks by tackling these core issues of secure and power aware/energy efficient routing.

10. References

1. Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., “Wireless Ad hoc Mobile Networks”, National Conference on Computing Communication and Technology, pp. 168-174, 2010
2. Samir R. Das, Charles E. Perkins and Elizabeth M. Royer, “Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks”
3. Ramanarayana Kandikattu, and Lillykutty Jacob, “Secure Internet Connectivity for Dynamic Source Routing (DSR) based Mobile Ad hoc Networks”, International Journal of Electronics, Circuits and Systems, pp. 40-45, 2007
4. David B. Johnson, David A. Maltz and Josh Broch, ” DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks”, http://www.monarch.cs.cmu.edu/
5. Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva, “A Performance Comarison of Multi-hop Wireless Ad Hoc Network Routing Protocols”, http://www.monarch.cs.cmu.edu/
6. Ashwani Kush, Phalguni Gupta, Ram Kumar, “Performance Comparison of Wireless Routing Protocols”, Journal of the CSI, Vol. 35 No.2, April-June 2005
7. Anne Aaron, Jie Weng, “Performance Comparison of Ad-hoc Routing Protocols for Networks with Node Energy Constraints”, available at http://ivms.stanford.edu
8. Charles Perkins, Elizabeth Royer, Samir Das, Mahesh Marina, “Performance of two on-demand Routing Protocols for Ad-hoc Networks”, IEEE Personal Communications, February 2001, pp.
9. C. Perkins, E. B. Royer, S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft”, RFC 3561, IETF Network Working Group, July 2003.
10. C. E. Perkins and E. M. Royer, “Ad-Hoc On Demand Distance Vector Routing”, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, 1999, pp. 90-100.
11. Internet Engineering Task Force (IETF) Mobile Ad Hoc Networks (MANET) Working Group Charter, Chaired by Joseph Macker and Scott Corson, http://www.ietf.org/ html.Charters/manet charter.html
12. Network Simulator, OPNET Modeler 10.5, available at http://www.opnet.com/
13. Ankur Khetrapal, “Routing Techniques for Mobile ad hoc Networks: a quantitative and qualitative analysis”, Proceedings of International Conference on Wireless Networks (ICWN' 06)
14. Elizabeth M. Royer and C.-K. Toh, “A Review of Current Routing Protocols for Ad- Hoc Mobile Wireless Networks”, IEEE Personal Communications Magazine, April 1999, pp.
15. A. Boukerche, “A performance comparison of routing protocols for ad hoc networks”, in proceedings 15th International Symposium on Parallel and distributed Processing, April 2001, pp. 1940-1946.
16. Ian Chakeres and Elizabeth Belding-Royer, “AODV Implementation Design and Performance Evaluation”, International Journal of Wireless and Mobile Computing, Issue 2/3, 2005.
17. Azizol Abdullah, Norlida Ramly, Abdullah Muhammed, Mohd Noor Derahman: Performance Comparison Study of Routing Protocols for Mobile Grid Environment, pp 82-88, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008

18. C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architecture and Protocols, ch. Routing Protocols for Ad Hoc Wireless Networks, pp. Prentice Hall Communications Engineering and Emerging Technologies Series, New Jersey: PrenticeHall Professional Technical Reference, 2004.
19. Irving,M., Taylor.G., and Hobson.P. (2004)