PERFORMANCE EVALUATION OF AOMDV AND IAOMDV UNDER PRETTY GOOD PRIVACY MODEL

Priyanka Bansal¹, Prof. Anuj K. Gupta²
¹Research Scholar, Department of Computer Science & Engineering, RIMT-IET, Punjab, India.
²Professor & Head, Department of Computer Science & Engineering, RIMT-IET, Punjab, India

Abstract: The routing protocols are used to boost or maximize network throughput, to maximize network lifetime, to maximize energy efficiency and to minimize delays. The network throughput is measured by packet delivery ratio and energy contribution is measured by routing overhead which is number or size of routing control packets. When the security model is applied, routing protocols behave differently. So, the effect of the overheads has to be analyzed in the current research work. The P.G.P. technique with AOMDV routing protocol will be applied to make it IAOMDV (Improved AOMDV) with the help of LOAD BALANCING. This strategy will make on demand protocols more secure. This study will useful for the protocols by making them more robust against attacks and also to standardize parameters for security in routing protocols. PKI and PGP play the vital role in terms of the safety measures. It is ease to maintain the safety of an established or fixed network but for an ambulatory (mobile) and dynamically changeable network it is highly difficult as malicious node can easily attack. Thus in the current research work, the safety measure with Public key infrastructures and its numerous types that can help to handle the security in the MANET will be focused by avoiding crucial Black Hole Attack and DDOS( Distributed Denial of Service) Attack by reducing the overheads.

Keywords: MANETs, PKI, PGP, AOMDV, Black Hole Attack, DDOS Attack, Security.

I. INTRODUCTION

Adhoc network is selection or collection of wireless mobile hops that forms a limited or kind of temporary network without any centralized mode of administration. In such kind of environment, it may be required for one of the mobile hop to enlist other hosts in forwarding the packet to its particular destination address due to restricted or limited transmission range of wireless network connections. Each of the mobile hop act not only as a hosts but also act as a router for transmitting packets for other mobile hops in the network that may not be in reach the forthright transmission spectrum of each other. Every node vigorously engage in an ad-hoc routing protocol that grants permission to it to discover multi-hop paths throughout the network to any other hop or node [1,11]. This concept of MANET is called infrastructure-less networking, since the mobile hops in network dynamically authorize routing among themselves to form their own network on the fly.

II. SECURITY REQUIREMENTS

In any fixed or dynamic wireless network, the security is integrated at three stages: prevention, detection and cure. The fundamental parts of prevention phase are authentication and authorization. The authentication is correlated with authenticating the engaged node, information and any other kind of important data like state of topology, counts of hop[12,13] etc. As authorization robustly is correlated with recognition. Whereas detection has the capability to consider misbehave carried out by hop or node in the network, the capability to take a remedial action after observing misbehave by a hop is described as cure. Distinct kind of possible intrusion or attacks on adhoc networks are respectively eavesdrop, compromised node, distorted message, replay message, fail to forward message, jamming signals etc. The pivotal point behind many of the desirable or possible attacks at any roll of security phases are authenticity, confidential, integrity, non repudiation, trustworthiness and availability.

Presently, there are considerable several proposals [2] available to solve these kinds of points or issues, but are not thoroughly comprehensive in nature as they spot or target particular threats separately. Therefore there is a vigorous requirement to have a productive security regime which can tend to take care of all the facets of security.

III. SECURITY THREATS

The widely two classes of network intrusion are active attacks and passive attacks.

A. Passive Attack

A passive attack doesn’t spoil the normal operation of protocol, but always tries to discover important information by listening to the traffic. Passive attacks [14] involve obtaining the fundamental routing information or crucial data by sniffing about the network. Such type of attacks is usually very difficult to detect and hence, defending against such type of attacks is complicated. The passive attacks are described as:

1. Traffic analysis: An attacker on the other hand in a more exquisite way, acquires intelligence by monitoring the transmission for patterns of communication. A substantial amount of crucial information is involved in
the flow of messages between communicating association parties.

B. Active Attack
An attack whereby an illegal party makes crucial changes to important messages or data streams. So, it is possible to find out this kind of malicious attack but it may not be correctable or curable. Active attacks therefore can take the form of one of four kinds of crucial masquerading, replay, message modification, black hole attack and denial-of-service. These malicious offensives are compiled as:

1. **Masquerading:** The attacker acts like an authorized user and thereby earns certainly unauthorized privileges.

2. **Replay:** The attacker carefully watches the broadcasts messages and resend messages as the appropriate (legitimate) user.

3. **Message modification:** The attacker modifies an appropriate (legitimate) message respectively by deletion, addition to, modification, or by reordering it.

4. **Black Hole Attack:** It is a type of attack in computer networking that forms the DOS attack in which router is supposed to broadcast packets instead of abandon them [10]. This generally occurs from a router that becomes settled from a number of different causes. Because packets are routinely released from lossy network, so packet drop attack is very challenging to uncover and prevent. The fake router can also accomplish this attack, for exemplar: by drop packets for particular network destination, at any time of day, a packet with every n packet or every second, or randomly selected portion of packets. So this is reasonably called gray hole attack. Also, if the vicious routers attempt to drop all packets that come in, then attack can actually be observed fairly as well as fast through common networking tools such as trace route. Further, even when other routers notice that settled router is dropping all traffic, they will begin to suppress that router from their forwarding tables and as a result no traffic will flow to attack. However, if malicious router begins to drop packets on definite time period or over every n packet, it is generally callous to detect as some traffic still flows across the network. Packet drop attack can frequently deploy to attack wireless adhoc networks. Wireless networks have much different architecture than that of typical wired network; a host cans newcast that it has the shortest path towards destination. By doing it, all traffic will be directed to particular host that has been compromised, and the host will be able to abolish packets. Also over Manet, hosts are specifically susceptible to collectively attacks where multiple hosts will become compromise and betray the other hosts on the network.

5. **Neighbor Attack:** The fundamental objective of the neighbor attack is to disrupt the multipath paths by making two hops that are in fact out of each other's transmission spectrum consider that they can transmit the data directly with each other [31]. If these two hops are part of network routing mesh, the join reply packages that they swap will be extinct because there is no actual existing connection and transmission between them. A neighbor attacker disrupts the routing protocol and doesn’t requirement to engage itself later in the package dropping mechanism, since the package will be vanished eventually due to the imitating links. At the time of obtaining packet, an intermediate node records its I.P. address in the packet since sending the packet to the later node. However, if attacker only delivers the packet even without recording its IP in the packet, it makes two hops that are not within the transmission spectrum of each other belief that they are neighbors, resulting in a disrupted route.

6. **DDOS (Distributed Denial of Service):** DDOS attack attempts to make system or network resource unavailable to its predetermined users. Although the means to carry out targets of this attack may vary, it usually consist of efforts to temporarily or indefinitely interrupted or suspended services of host connected to Internet. Criminals of these attacks typically target large websites or services hosted on high-profile cyberspace servers such as the netbanking and credit card payment gateways, and root name servers. This approach has now extensive use in some games, used by server owners, or cranky competitors on games. Progressively, these attacks have also used as a form of resistance. This is a tool for registering disagreement. The Richard Stallman has said that DDOS is form of 'Internet Street Protests'. This term is usually used relating to computer networks, but it is not limited to this field; for exemplar, it can even used in reference to Central Processing Unit resource management.

One of the common way of attack involves saturating the target machine with outside transmissions requests alot so that it can’t respond to legitimate traffic and responds so slowly as to be accomplished essentially unavailable. These types of attacks usually lead to server overload. In usual terms, DOS attacks are achieved by either force the targeted computer to reset or by exhausting its resources so that it can no longer provides its predetermined services or obstructing the communication media.
between the predetermined user and the sufferer so that they can no longer do communication adequately. Denial-of-service attacks are considered to be the violations of the Cyberspace Architecture Board’s and cyberspace proper use policy & also offend the acceptable use the policies of virtually all the I.S.P. They commonly constitute the violations of laws of the individual nations. The emanation or consequences of these types of attacks included, but are not only defined or limited to, failure of proprietary and crucial information, legal and recovery costs and loss of other network services. Adhoc networks face many type of issues as well as problems due to which a persistent and secured network flow becomes very tough challenging task. Some of the issues or problems correlated are given below.

1) Ad-Hoc networks mainly being wireless have defined or limited band-width as compare to wired networks. The smaller package of packets is available to transmit data and it furthermore restricted to use the less number of bits for security as well as safety purposes. It has been predicted that this constraint will be eased with the improvement as well as advancement of hardware in future as well as in further work.

2) The engaged hops of Ad-Hoc networks generally are mobile devices which have very finite capabilities likely processing power, size of memory and backup of battery. It makes the effective use of digital signature [3], as security part and less convenient as digital signatures are computation demanding. The usage of digital signatures may also be consumed considerably memory if digital signatures are affixed by each node that dispatch the packet to its destination address. Moreover PKI [4] framework is not practical able in case of Ad-Hoc [15] type of networks. Other kind of problem with usage of digital signature is to keep maintaining a certificate revocation list (CRL), in the unavailability of a central server. The resolution to this problem can be concluded by using some security measures only.

3) The usage of hashing techniques although offer efficiently security methods but have been used somewhat less. The hashing mechanism like MAC [3], HMAC [3], one way hash chains [8] etc. have mostly used for verifying as well as authenticating routing and crucial information. The effective performance of hashing techniques depends mainly by this way; the collisions have been looked upon.

IV. AOMDV ROUTING PROTOCOL REVIEW

AOMDV Routing Protocol [9] is one of the most currently used Ad-Hoc routing protocol. This reactive routing protocol based on the DSDV. AOMDV protocol is created for network systems with tens to thousands of mobile hops. The main concept in AOMDV is to compute or produce multiple paths during route discovery process. It is created mainly for highly dynamic ad-hoc type of networks where the link failures as well as route breaks take place usually. When single path protocols like reactive routing protocol such as AODV is when used in such type of networks, a new route discovery is required in response to each route break. Every route discovery is correlated with high overhead and latency. This inability as well as inefficiency can be evaded or avoided by having the numerous (multiple) redundant paths availability. The AOMDV protocol has two phases:

1. A route updating rule to create and manage multiple loop free paths at every hop.
2. A distributed protocol to find out the node-disjoint paths that is route discovery.

In AOMDV a new route discovery is required only when all the paths leads to the destination break. Main characteristics of the AOMDV protocol is the usage of routing information that is earlier available in the basic AODV protocol as much as possible. Therefore little additional overhead is enforced for the computation of multiple paths.

A. Route Discovery

The route discovery process has broadly two aspects: route request and route reply aspect. The route discovery process computes the multiple loop free paths. The route discovery process will be started only when a route is desired by a source hop and there is no data about the route in its respective routing table. Firstly, source hop set up an RREQ and then deluge the packet to the networks. The RREQ’s are propagated to neighbours within the source’s transmission spectrum. They also renounce the packets to their respective neighbours. The operation is replicated till the destination accepts the RREQ. When an intermediate node accepts the RREQ, it performs the following procedure:

1. When an intermediary hop gets the information of RREQ, either it transmit the route reply if the hop is the destination, or it renounce the RREQ to it neighbours.
2. The hop scans the required information from the RREQ.

In order to transfer route reply packets to the source hop, the hop makes a reverse path to the source hop. The hop
will embed the path to its numerous multiple path lists. Otherwise, the hop will avoid the path and abandon the RREQ.

Link failures in ad-hoc networks are induced by mobility, congestion, packet collisions, node or hop failures etc. The link layer in the AOMDV protocol evaluated from IEEE 802.11 is utilized to detect or reveal link failures. If a hop delivers packets along the broken link, it will be accepted or received by a link layer feedback. When a hop reveals a link break, it broadcasts as well as announces route error (RERR) packets to its neighbours. The neighbours then rebroadcast and renounce the packets until the entire source hops get as well as receive the packets. If a source hop accepts the RRER, it will discard each entry in its respective routing table that takes the usage of the broken link. As compare from single-path routing protocols, the routes having error packets should consist of the crucial information not only about the broken primary paths but even the broken backup routes. When the source originated hop gets the RERR’s, it discards all smashed routing entries and utilizes the shortest backup paths as initial paths. The source hop originates a route discovery process where all the backup paths are broken.

B. Benefits and Limitations
AOMDV is on demand reactive routing protocol which determines the route as and when needed by sending packets to its neighbors. AOMDV choose the most optimum path from available paths between source node and destination node. The optimization criteria can be shortest and least congested path.

V. IMPACT of ATTACKS
Black hole attack and DDOS attack has been implemented in an ns2 simulator [22]. Impact of these attacks on AOMDV protocol will be compared with AOMDV protocol without attacks. The problem formulation is reviewed emphatically by compiling data, various experiments and simulation which gives some results then these results are evaluated and opinions and judgments are made on this criterion. To analyze the effective performance as well as results of a protocol for Adhoc network, it is significant to evaluate it under practical conditions, especially including the movement of mobile-hops. The simulation demands to initiate traffic and mobility model for performance evaluation process. The impact of attacks on AOMDV protocol is very critical. So, it must be improved by proposed technique i.e. Pretty Good Privacy Key Management.

VI. SECURE ROUTING
The routing protocols [5, 6, and 7] within ad-hoc networks are more susceptible to attacks as every device performs as a relay. Any kind of interference with the routing information can denial or compromise the entire network. An attacker can introduce fraud information within routing messages or review elderly logged or stored information. The main objective is to safeguard any vital information or behavior that can amend or causing a change to the routing tables on co-operating hops convoluted in ad-hoc routing protocol [16]. For the completeness, timeliness and ordering are combined to the list of advisable security features that can wipe out the risk of attacks against routing protocols.

A. Proposed Technique
There are a number of proposed solutions for security authentication and key management in MANET. Proposed authentication architecture for MANET, describing the formats of messages, together with protocols which achieve authentication as in the architecture can accommodate different authentication schemes. One quite useful approach to the problem comprises PGP-based schemes.

B. Flow diagram

C. PGP-Based Solutions
The ‘Public Key Infrastructure’ (PKI) is the most scalable form of key management. Several different PKI techniques exist, such as SPKI, PGP and X.509. Varied modes of these PKI techniques have been recommended for usage in Adhoc networks. Ref. [20] on security architecture proposes the use of a group-oriented PKI for large group formation. The pioneer of the faction performed as a ‘Certificate Authority’ (CA), which releases pioneer membership certificates. These are said to be SPKI-style certificates. They certify that the public key in the certificate exist to a pioneer member. However, this is not useful for two-party
communications or non-group-oriented tasks. On self-organized public key certificate management works like PGP [19], which grant permission to users for creation, storage, distribution, and revoke their public keys without the help of any trusted authority or fixed server.

D. Certification

Public key certificate is the prerequisite for proving identity authentication between mobile ad hoc networks (MANET) nodes. Though MANET are of dynamic topologies and have infrastructure-less property, that carry the challengers for public key verification, similarly in hierarchical Public Key Infrastructure (PKI) in MANET [17]. The outcomes in terms of certificate convergence span of time. This model needs more specific protocol for formal verification and analysis.

MANET is pervaded by matters like unreliability of wireless media, unreliable connectivity, host mobility and infrastructure less [18]. However, maybe, a necessary facet of such networks is the issue of safety measure. The computational load and intricacy involved in this environment are robust subject to the dynamic nature of network topology, [21] especially the constraint by the hops feasible resources. Therefore, key management and authentication are fundamental facet for safety measure in MANET and thus they should not be fragile. The given model is only for small scale networks using PGP Technique but model is not plentiful for scalable network.

In Dynamic networks, protocols are used like AODV, AOMDV etc. The performance of protocols should be analyzed in terms performance matrices [2]. PKI is a new security technology, its role is to provide information security services, can use it to ensure that the network information security [4]. This article describes the theoretical basis of PKI and related technologies and concepts, analysis and comparison of PKI-based trust model: hierarchical trust model, peer trust model, network trust model, hybrid trust model. Analyzes the current PKI trust management and related lack of trust management system, given the open network environment, trust management system should have features.

Certificate-based cryptography and ID-based cryptography have been organized under distinct theoretical backgrounds and they have their own pros and cons, but there have been lean tasks which seek to contribute a uncommon private key issuing protocol in the single-authority multiple-observer (SAMO) model which can weaken the user authentication load alot more, but these strategies are subject matter to various attacks due to the lack of valid authentication of protocol messages. In this research, these two issues can be resolved by linking certificate-based and ID-based cryptography. In the proposed scheme, certificate is circulated to user for user-chosen public key and ID-based private key is issued to user via a private key issuing protocol. In the private key issuing protocol user is authenticated and validated by using the certificate and protocol messages are blinded by usage of the certified public key of the user, thus the private key issuing protocol becomes private and also verifiable, which clarifies the authentication problem[21]. Then present the conception of unified public key infrastructure (UPKI) in which both certificate-based and ID-based cryptosystems are granted to users in a single frame. It has also shown that if interactions between users are mainly carried out using ID-based cryptography, then users need not to handle other end users’ certificates, which is an extreme efficiency gain than traditional PKI.

Adhoc network is selection or collection of wireless mobile hops that forms a limited or kind of temporary network without any centralized mode of administration. In such kind of environment, it may be required for one of the mobile hop to enlist other hosts in forwarding the packet to its particular destination address due to restricted or limited transmission range of wireless network connections [15] . With these network properties, security has become a essential matter for researchers to expedient scientific threats to market convenience in term of confidential, authenticity, integrity, availability, access control, and non-repudiation. So, a powerful tool for acquiring security is required, the Key Management becomes a vital element in MANET security by introducing an relevant secure method for conducting cryptographic keying matters. The Key Management outlook includes key generation, key distribution, and key maintenance. Main objective of this research is to figure out and to present a recent review on different research works on Key Management in MANETs.

This system does not assign specific missions to a node or subset of nodes (i.e. all the nodes have the same role). In this system, like in, users’ public and private keys are formed by the users themselves. It is counterfeited that every genuine user owned a specific mobile hop. Hence the same identifier is used for the user and the other node (i.e. both being denoted by v) [21]. Unlike in PGP, where certificates are mainly stored in centralized certificate repositories, certificates in proposed system are reserved and assigned by the hops in a totally self-organized manner. Every certificate is issued with a defined validity time and therefore having its issuing and times expiration. Since a certificate ceases, its issuer releases the updated version of the look-alike certificate, which have an extensive expiration time. This updated version is termed as the certificate update. Every hop
periodically issues certificate updates, since its owner examine that the user-key bindings have in these certificates are appropriate. In this system, key authentication is achieved through chains of public-key certificates in the consecutive way: When a end-user \(v\) wants to have the access of the public key of other end-user \(u\), he obtains a chain of persuasive public-key certificates like:

1. The first certificate of chain can be directly go through by \(v\), by usage of a public key that \(v\) holds and have trust on it (e.g. her own public key).
2. Every resting certificate can be checked by using the public key have in the earlier certificate of the chain.
3. The last certificate hence involves the public key of the target user \(v\).

In this system, the certificate revocation is an important mechanism. It enables two types of certificate revocation: explicit and implicit. The issuer explicitly renounces a certificate by issuing a revocation statement and by forwarding it to the hops which holds the certificate in question. The implicit revocation depends on the expiration span of time hold in the certificates. Each one certificate whose expiration span of time passes is implicitly revoked; this secondary system is genuine, but there is requirement of some loose time synchronization of the hops. The quest for security in MANET led a PGP type PKI. In PGP, any kind of hop can release a certificate and it allows a complete distributed architectonics as such, besides from the central repository, which obtains these certificates. It introduces a strategy to avert the requirement for a central repository of certificates in the PGP system [21, 23]. This strategy includes every hop conformity mini-repositories, which obtains all the certificates that the hop releases and all the certificates released on it. When hops \(A\) and \(B\) confirmed, they meld their mini-repositories. The repositories are formulated corresponding to the ‘Shortcut Hunter algorithm [25]. This algorithm formulates repositories such that the two hops melding repositories have a large feasibility of founding a chain of certificates among them if one remains. This strategy is very helpful in a civilian kind of environment where delegation of trust through a number of hops is acceptable. Let the notation \(A \rightarrow B\) mean that \(A\) trusts \(B\). Then what the implications \(A \rightarrow B, B \rightarrow C, C \rightarrow D\) and \(D \rightarrow E\) signify is that \(A\) chooses to trust \(E\) i.e. \(A \rightarrow E\). A different access is the usage of Certificate Authority (CA) to release certificates. CA is as third party trusted by all in systems, which effectively reduces the requirement for a repository of certificates. Rather than founding a certificate linking \(A \rightarrow B \rightarrow C \rightarrow D \rightarrow E\), one can easily restores the certificate \(A \rightarrow E\). Therefore, CA can be view as a one-hop shortcut through the web of trust. The main problem with this is the CA that must be trusted as well as loyal by all and becomes a single point of failure in the event of an attack.

E. Methodology behind Improvement of AOMDV (LOAD BALANCE and Congestion Control)

Balancing load to avoid congestion inside novel scheme of flow control is actually performed by creating a Cycle on a node where the congestion probability is high i.e. at near sink node to find all those nearer nodes where buffer occupancy is high. Near sink node and nodes nearer to it contains the routing table including information about its own I.P. address, I.P. address of nearer neighbor nodes, distance between the nodes, & queue length of each node as shown in Fig. 2.

The dynamic nature of wireless sensor network cause the topology to automatically change due to change in topology each node automatically updates its information in its own routing table & the routing table of the nearer node regarding its buffer length, its distance from other nodes, its I.P. address.

There are following steps to be followed during this process:

1. Firstly the Hop-by-Hop algorithm is to be implemented on congestion affected node. This algorithm check’s the routing table of congestion affected node to find all the nodes nearer to it with minimum response length time i.e. it must have maximum buffer occupancy to accommodate the load of congestion affected node.
2. After finding the node with free buffer space Hop-by-Hop algorithm make that node as the child node of the congestion affected node and the alternate routes from the congestion affected node to the nearer node will become active to transmit data so as to utilize its buffer space.
3. As soon as the time period during which child node receives the packets in its buffer space from the congestion affected parent node it will store them in its buffer for a short time interval.
4. On receiving the packets from congestion affected node by the nearer node at the same time this node will immediately implement the Hop-to-Destination algorithm to forward the packets to the destination i.e. sink Node base.
station within the finite amount of time. The scenario for this whole process is shown in Fig. 3.

![Figure 3: Node’s with free space transmitting packet to sink](image)

**VII. SIMULATIONS AND RESULTS**

**A. Simulation Environment**

Simulations are done to compare the routing protocols i.e. AOMDV and proposed IAOMDV. IAOMDV routing protocol with P.G.P. model and Load Balancing technique will be compared with AOMDV routing protocol. Simulator NS-2(2.34) is used [24] for performance comparison. NS contributes significant support for simulation of TCP, routing, multicast and multipath protocols over wired and wireless (local and satellite) networks. It work on network layer and inform about link breakage. The implementation of the protocol has been done using C++ language in the backend and TCL language in the frontend. TCL (Tool Command Language) is compatible with C++ programming language. Interpretation is based upon two files trace files and nam files are to be generated. Network Animator (.nam) file, records all the visual events that happened during the simulation. Trace files (.tr), records the entire network event that occur during the simulation. And file is post analyzed with the help of awk scripts.

**B. Traffic Scenario**

Table 1. Shows Traffic Scenario

<table>
<thead>
<tr>
<th>PARAMETRES</th>
<th>VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIMULATOR</td>
<td>NS2.34</td>
</tr>
<tr>
<td>ROUTING PROTOCOL</td>
<td>AOMDV, IAOMDV</td>
</tr>
<tr>
<td>ATTACKS</td>
<td>BLACK HOLE ATTACK, NEIGHBOR ATTACK,</td>
</tr>
<tr>
<td>SECURITY</td>
<td>PGP</td>
</tr>
<tr>
<td>CHANNEL</td>
<td>WIRELESS CHANNEL</td>
</tr>
<tr>
<td>MEDIA ACCESS PROTOCOL</td>
<td>IEEE 802.11b</td>
</tr>
<tr>
<td>AREA</td>
<td>1000mX1000 m</td>
</tr>
<tr>
<td>TRAFFIC TYPE</td>
<td>CBR, TCP</td>
</tr>
<tr>
<td>VELOCITY</td>
<td>8.32m/sec</td>
</tr>
<tr>
<td>PACKET SIZE</td>
<td>512</td>
</tr>
<tr>
<td>NUMBER OF NODES</td>
<td>50, 80, 100</td>
</tr>
<tr>
<td>SIMULATION TIME</td>
<td>50 sec</td>
</tr>
<tr>
<td>PROPAGATION MODEL</td>
<td>TWO-RAY GROUND</td>
</tr>
<tr>
<td>PAUSE TIME</td>
<td>50</td>
</tr>
<tr>
<td>MOBILITY MODEL</td>
<td>RANDOM WAY-POINT</td>
</tr>
<tr>
<td>ANTENNA TYPE</td>
<td>OMNI-ANTENNA</td>
</tr>
</tbody>
</table>

**C. Simulating Results and Analysis**

Following performance metrics are used to figure out the two routing protocols:

1. **Packet Delivery Ratio (PDF):** It is the ratio of the packets received by destination to those generated by the sources. CBR traffic type is used by source. It specifies the packet loss rate, which restricts as well as limit the maximum throughput of the network. The routing protocol which have better PDR, the more complete and correct. This reflects the usefulness of the protocol. And provide good performance.
2. **End to End Delay:** Average end-to-end delay is the average time it taken by the packet to reach to destination in seconds.
3. **Throughput:** No. of packet passing through the network in a unit of time. It is measure in kbps.

![Figure 10: Throughput Graph of 50 Nodes](image1)

![Figure 11: Throughput Graph of 80 Nodes](image2)

![Figure 12: Throughput Graph of 100 Nodes](image3)

**D. Simulations Result Table**

<table>
<thead>
<tr>
<th>ROUTING</th>
<th>AVERAGE EEDELAY</th>
<th>AVERAGE PDF</th>
<th>AVERAGE THROUGHPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOMDV</td>
<td>30.12 ms</td>
<td>0.95 %</td>
<td>357.22 kbps</td>
</tr>
<tr>
<td>AOMDV with Attacks</td>
<td>80.6 ms</td>
<td>0.71 %</td>
<td>347.85 kbps</td>
</tr>
<tr>
<td>IAOMDV</td>
<td>29.59 ms</td>
<td>0.97 %</td>
<td>450.05 kbps</td>
</tr>
</tbody>
</table>

**E. Comparison**

![Figure 13: End to End Delay Comparison](image4)

![Figure 14: Packet Delivery Fraction Comparison](image5)
Multipath routing techniques used in reactive protocols to obtain fast and effective recovery from route failures in highly dynamic Ad-hoc networks. In the thesis work, an Improved AOMDV routing protocol that extend the AOMDV protocol for enhancement the security by avoiding black hole attacks and DDOS attacks using P.G.P. model. Simulation results show that the throughput, packet delivery fraction IAOMDV is more as compare to AOMDV. Also overhead of IAOMDV is lesser than AOMDV. This is because IAOMDV has more security and load balancing to reduce overheads. In future, these techniques may be implemented with modified version of AOMDV and also with multicast routing protocols such as the On-demand Multicast Routing Protocol (ODMRP) and result for the different performance matrices be scrutinize. This facet can be one field for future research work.

ACKNOWLEDGMENT

This work is done in Department of Computer Science & Engineering, RIMT-IET, Mandi Gobindgarh, and Punjab, India. I would like to express my sincere gratitude to the supervisor of this work, Associate Professor & H.O.D. Mr. Anuj K. Gupta who gave me this wonderful opportunity to work under him and to provide me with valuable guidance and necessary support throughout the Master course. Without their support, I could not finish my Master degree studies.


