A Performance Comparison of Routing Protocols and Cryptography Based Secured Routing Protocol in MANET's

Navneet Kumar [1], Prof. S. R. Yadav[2]
[1] PG Scholar, MITS, Bhopal (India), [2] Head PG, CSE, MITS, Bhopal (India)

Abstract – Networks are being used in various areas and the mobile ad-hoc network (MANET) is the network in Laptops, smart phones. MANET is a dynamic network without the fixed infrastructure due to their wireless nature and topology and changes due to their dynamic nature. In MANET various routing protocols are used, AODV routing protocol is one of them and the AODV has the different characteristics, AODV is the reactive routing protocol and disadvantages of DSDV routing protocol is overcome by AODV. The work is concentrated primarily on the provision of security in the On-demand routing protocols like Ad hoc On Demand Vector (AODV) and Dynamic Source Routing (DSR) since they are efficient for routing in large ad hoc networks and they initiate and maintain the routes that are currently needed. The work proposes the application of Dual Hash Authentication Technique (DHT) in association with Self-Healing and Optimizing Routing Technique (SHORT) in AODV. In Dual Hash Authentication, one hash function is used to authenticate the received routing packets and the other one is used to prevent the current nodes modifying the routing information themselves. SHORT helps all the neighboring nodes to monitor the route and when a better local sub-path is available.

Keywords -Mobile ad-hoc network, NS2, Routing protocol, RC6, Security.

1. INTRODUCTION

To meet the need for a fast and reliable information exchange, communication networks have become an integral part of our society. The success of any organization largely depends on its ability to communicate. Ad hoc wireless networks will enhance communication capability significantly by providing connectivity from anywhere at any time. In recent years, Mobile Ad hoc Networks (MANETs) have seen widespread applications in commercial, domestic and strategic areas and with more focus on their security.

As the field of communications networks continues to evolve, a need for wireless connectivity and mobile communication is rapidly emerging. In general, wireless communication networks provide wireless mobile access to an existing communication network with a well-defined infrastructure. Ad hoc wireless networks provide mobile communication capability to satisfy a need of a temporary nature and without the existence of any well-defined infrastructure. Such networks have many potential applications including the Disaster recovery situations, Defense applications (army, navy, air force), Healthcare, Academic institutions, Corporate conventions/meetings.

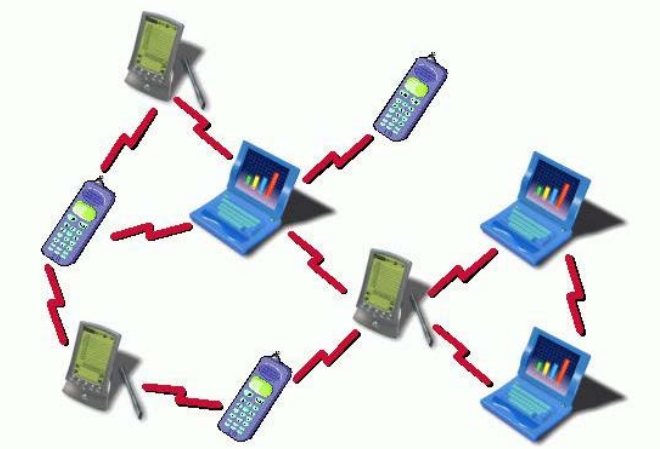

Figure 1: Mobile Ad hoc Network

For all those reasons, mobile ad hoc networking is one of the more innovative and challenging areas of wireless networking and this technology promises to become increasingly present in everybody's life. However, before an ad hoc network becomes a commodity, several security issues must first be resolved. On one hand, the security-sensitive applications of ad hoc networks require a high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. Though security mechanisms for ad hoc networks are available, because of easy deployment, the need for this network increases for many applications and more number of users are involved, the scope for malicious users also increases. Hence the available security mechanisms are not sufficient and for every kind of routing protocols proper security mechanism have to be incorporated.

1.2 Requirements of MANET

In mobile ad hoc networks, nodes act as both routers and terminals. For the lack of routing infrastructure, the nodes have to cooperate to communicate. Cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding. Misbehaviour means aberration from normal routing and forwarding behaviour. Depending on the proportion of misbehaving nodes and their specific strategies, packet loss increases, nodes can be denied service, network throughput can be severely degraded and the network can be partitioned. These detrimental effects of misbehaviour can endanger the functioning of the entire network.

2. SYSTEM MODEL

Ad hoc networks come into existence when two or more wireless mobile nodes agree to pass packets for each other. Ad hoc on demand distance vector (AODV) is one of the frequently used routing protocol and network is established. Network popularity has motivated the development of Mobile Ad hoc Networks (MANETs). MANETs provide communication between the nodes in the network without the presence of a central node which is normally found in the cellular and other networks. Fast changing network is created by this system. Different attacks that can be possible on AODV will be analysed. Normal AODV performance will be improved. We are proposing an extended version to secure AODV protocol and the working of AODV routing protocol studied.

In this paper we are going to decide evaluation parameters or performance parameters and attack analysis will be done. Cryptographic based security solution provided and the analysis of proposed protocol or algorithm in term of decided evaluation parameters will be performed. Using cryptographic technique AODV's security with network performance improved. Performance factor and security factor is checked by network simulator NS2. NS2 contains or else it is based on two languages they are OTCL and C++, OTCL is the object oriented extended version of TCL that is tool command language. The TCL generates the two files trace file and nam file. The nam file contains the network animator and trace file contains the information about sent packets and received packets, timing information. The packet delivery ratio, throughput, energy, delay is calculated by the awk script. In AODV if it is attacked by some attacks then the evaluation parameters such as PDR, throughput, delay, and energy get affected. The description about the various attacks is given below.

Layer	Security issue
Application Layer	Detecting And Preventing Viruses, Worms, Malicious Codes, And Application Abuses.
Transport Layer	Authentication And Securing End-To-End Communications Through Data Encryption.
Network layer	Protecting The Ad Hoc Routing And Forwarding Protocols.
Link Layer	Protecting The Wireless Mac Protocol And Providing Link- Layer Security Support
Physical Layer	Preventing Signal Jamming Denial-Of-Service Attacks.

A. Types of Attacks

There are mainly two types of attack they are internal attacks And external attacks.

Internal attacks: The attacker acts one of the nodes from the Containing nodes and gains direct access to the network and Can do the malicious activity.

External attacks: The attacker attacks from outside the Network in this type, due to congestion in the network traffic By propagating non meaningful messages throughout the Network , thereby disturb the entire communication of the network.

I. Impersonation

This type of attack is fall in the category of the most severe attacks. The attacker can act as an innocent node and join the network in this type of attack. Similar way, when several this type of nodes join the network, they gain the full control of the network and conduct malicious behavior. They spread fake routing information and they also gain access to confidential information. A network is vulnerable to such attacks if it does not employ a proper authentication mechanism.

2. Denial of Service

This type of attack is first making sure that a specific node is not available for service. So the entire service of the network might be disturbed due to this attack.

3. Eavesdropping

The main goal of the attacker is to get some private information in this type of attack, while it is being transferred

from one node to the other. This attack is very much complex to find out and the secret information like private and public key password etc. of the nodes can get compromised due to this attack.

4. Black hole attack

A black hole is created with the opponent at the main Centre. The opponent traps the traffic of the network close to a compromised in this type of attack. Basically the attacker offers an attractive path to the neighboring nodes. This attack can also be paired with other attacks like packets dropping, denial of service, replay of knowledge, selective forwarding.

5. Wormhole attack

Here the opponent connects two distant parts of the network and convey messages received in different part of the network to the other. A lower latency link is used to pass the messages in this type of network.

6. Sybil attack

In this type of an attack, a particular node in the network tries to have several different fake identities. Thus this way helps the malicious node to gain more and more specific information about the network. The validness of fauIt tolerant schemes like; muItipath topology in routing, distributed storage, maintenance has a great decrease.

B. Cryptography

The technique we are using here is Cryptography technique. The simplified meaning of cryptography is encryption. Encryption is the process of coding the information in such away that its meaning is hidden. The reverse process of encryption is decryption. Encryption and Decryption uses a key. The coding is done in such a way that decryption is done only when proper key is known. Now a day's cryptography is not only encryption and decryption, it is developed to provide

1.Confidentiality: The prevention of unauthorized disclosure of information.

2.Integrity: The prevention of erroneous modification of information.

3.Availability : The prevention of unauthorized withholding of information or resources.

4.Authentication : The process of veritying that users are who they claim to be when logging onto a system.

5.Authorization : The process of allowing only authorized users' access to sensitive information. Privacy ensures that the only the sender and intended recipient of an encrypted message can read the contents of the message that are transmitted from one place to another and cannot be understood by any intermediate parties that may have intercepted the data stream. Non-repudiation provides a method to guarantee that a party to a transaction cannot falsely claim that they did not participate in that transaction. Cryptographic systems are characterized along three independent dimensions:

(1) The type of operations used for transforming plaintext to ciphertext.

(2)The number of keys used.

(3)The way in which the plaintext is processed.

3. PREVIOUS WORK

[1] Latha Tamilselvan, V Sankaranarayanan [2] gives the solution to remove the black hole attack and improvement of the AODV routing protocol but in this paper they had given a table in which the reliability of the node is shown but what happens in this case is that the if the level of node is 0 then that node is discarded from the network because the network Consider that node as black hole node, and also this network has the delay in processing.

[2] In this paper [2] as the main aim is to remove the black hole attack from the AODV. But in this paper what happens the delay in the normal AODV is less and when the AODV is attacked by the black hole node the delay increases that should not be happen in case of the attack.

[3] Deswal and Singh [3] created an enhanced version of the SAODV protocol that includes password security for each of the routing nodes and routing tables that are updated based on timeliness.

[4] In this paper [4], they investigated some of the existing

solutions for black hole attacks. They proposed a nove) approach for detecting and preventing black hole attacks and securing a route to the destination in an efficient manner. The simulation results showed that the SRD-AODV mechanism greatly increases the packet delivery ratio for three types of

environments with node mobility when black hole attacks are occurring on the network

.4. PROPOSED METHODOLOGY

The nodes in an ad hoc network also function as routers that

discover and maintain routes to other nodes in the network. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner (Hongmei Deng, Wei Li, and Dharma P. Agarwal, 2002). If routing is misdirected, the entire network will be paralyzed. Thus, routing security playsan important role in the security of the whole network. This chapter discusses about how routing is done in the routing protocols AODV and DSR. It also discusses about the implementation of the proposed security mechanism Dual Hash Authentication and its performance in the above two routing protocols.

4.1 ROUTING PROTOCOLS

4.1.1 AODV Routing Protocol

AODV is an important on-demand routing protocol that creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. It broadcasts a route request (RREQ) packet (Figure 3.1) to its neighbours and so on, until either the destination or an intermediate node with a fresh route to the destination is located. In this process, the intermediate node can reply to the RREQ packet only if it has a fresh route to the destination.

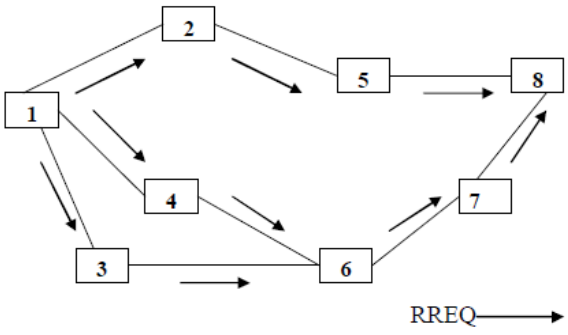

Figure 3.1 Propagation of RREQ in AODV 3.2.2 DSR Protocol

Once the RREQ reaches the destination or an intermediate node with a fresh route, the destination or intermediate node responds by unicasting a route reply (RREP) packet (Figure 3.2) back to the neighbour from which it first received the RREQ. After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired.

The Dynamic Source Routing (DSR) protocol proposed by Johnson and Maltz (1996) is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This rout request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination.

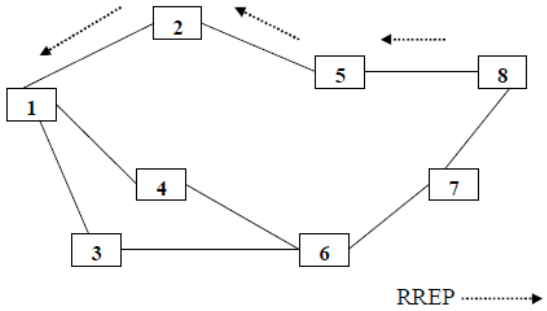

Figure 3.2 Propagation of RREP in AODV

If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record. A route reply is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. If the node generating the route reply is the destination, it

places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply.

4.1.2 DSR Protocol

The Dynamic Source Routing (DSR) protocol proposed by Johnson and Maltz (1996) is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet.

On the other hand, if the node does not have such a route, it Initiates route discovery by broadcasting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet Checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record.

3.2.3 Dual Hash Authentication in AODV and DSR

The Fast and Efficient Hash function is adopted to authenticate routing information instead of digital signatures (Kimaya Sanzgiri et al, 2005) under the reasonable assumption that no two compromised nodes are colluding and are within two hops between each other. In this dual hash authentication, one is used to authenticate the received routing packets and other is used to prevent the current nodes modifying the routing information themselves (Xinjun Du Ying, et al, 2003). If some compromised node modified the routing information, its neighbouring nodes can detect the misbehaviour immediately. In an initial phase each node makes use of the management of local node group to distribute the common secret with its two hop node group.

5. SIMULATION/EXPERIMENTAL RESULTS

In this section we describe our simulation environment and performance metrics.

5.1 Simulation Environment

For our simulations we used ns-2.34 [9], a packet-level discrete event simulator. Ns-2.34 includes the simulation model for mobile ad hoc networks. The model includes a physical layer, an 802.11 MAC layer, and a data link layer [8]. The wireless channel capacity is 2Mb/sec. As mentioned earlier, we performed our study with AODV and modified AODV.

The default overall buffer size of the scheduler of each node is 64 packets. The buffer is shared by multiple queues when the scheduler maintains multiple queues. The AODV protocol implementation in ns-2.34 also maintains a buffer of 64 packets used during route discovery. The maximum waiting time in the send buffer during route discovery is 30 seconds. If a packet remains in the send buffer for over 30 seconds, the packet is dropped.

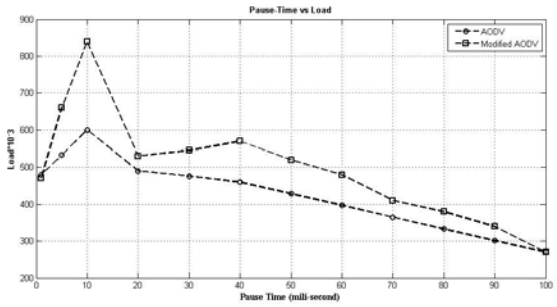

Figure:2 Network load Vs Pause Time

We use 50 mobile nodes in a rectangular grid of dimensions 100m x 300m. We ran each simulation for 900 seconds. We use the random waypoint model because it is the most widely used mobility model in previous studies [3]. In this model, a node decides to move to a random location within the grid. When it reaches that out of range, it pauses for a fixed amount of time, possibly zero seconds, and then it moves to another random location. The maximum allowed speed for a node is 20 meters per second. We use a constant bit rate (CBR) source as the data source for each node. Each source node transmits packets at a certain rate, with a packet size of 512 bytes. We choose source and destination nodes randomly among all nodes.

The communication patterns are peer-to-peer, and connections were initiated at random times between 0 and 180 seconds. We vary the traffic load and the degree of mobility in the simulations. We vary traffic load by changing

the number of sources or the packet sending rate. We control the degree of mobility through the pause time.

We use pause times of 0, 30, 60, 120, 300, 600, and 900 seconds. A pause time of 0 seconds implies constant movement, whereas 900 seconds implies no movement at all since our simulations run for 900 seconds. A movement scenario arranges the movement and the position of the nodes according to the random waypoint model. Because the simulation results depend on the movement scenarios, we averaged simulation results over four different movement scenarios for each data point.

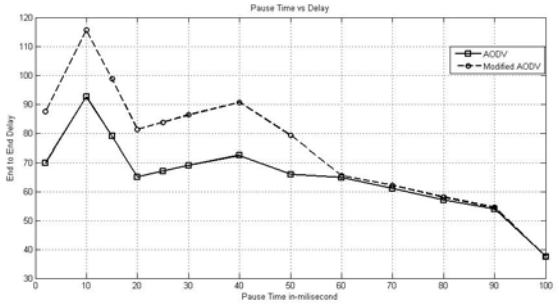

Figure:3 End to end delay Vs Pause Time

5.2 Performance Matrices

We use the following performance metrics to evaluate the Effect of each scheduling algorithm: Average end to end delay: This is the average overall delay for a packet to travel from a source node to a destination node.

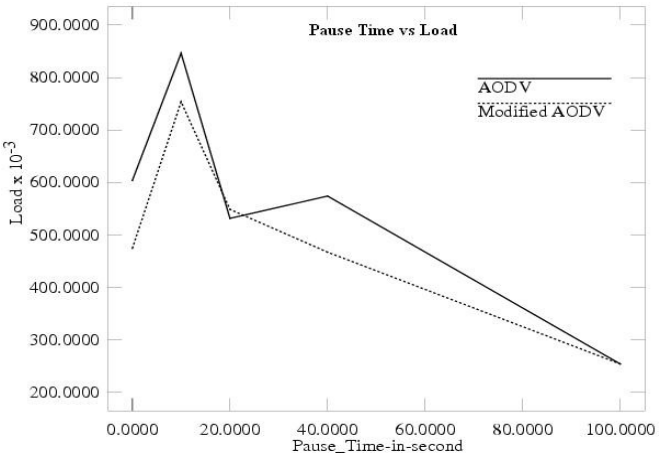

Figure: 4 Normalized load (AODV and Modified AODV)

This includes the route discovery time, the queuing delay at a node, the retransmission delay at the MAC layer, and the propagation and transfer time in the wireless channel. Average load: This is the average number of data packets received by the destination node per second.

We also measured routing overhead, defined as the average ratio of routing-related transmissions to data transmissions. The transmission in each hop is counted when a node sends or forwards a packet. Since the routing overhead is not affected considerably the choice of scheduling algorithms (the maximum difference of the routing overhead among scheduling algorithms is less than 0.05), we do not present it here. The performance result of AODV and modified AODV routing protocol as shown in

figure: 3 and show the result between load and pause during connection establishment process. In figure: 4 end to end delay decreases with respect to pause time during route maintenance process. When mobile nodes sends the data packets then intermediate node forward the packet to its neighbor node and figure: 4 show the packet delivery ratio and pause time. Remaining result shown in figure: 5 and it show the explanation of simulated result. Here result 2 to outcomes from network simulator 2.34 [14].

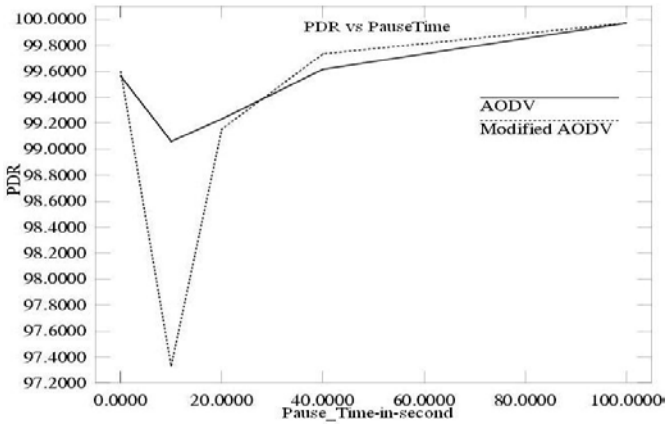

Figure: 5 Packet Delivery Ratio (AODV and Modified AODV)

we are using weight hop based packet scheduling for AODV routing protocol. We evaluate the effect of different scheduling algorithms for AODV and modified AODV. Here mobility and routing protocols show the composition of packets in queue. During low mobility, the average delay is dominated by network congestion due to data traffic. During high mobility, it is dominated by route changes in the simulation results. Our scheduling algorithms that give higher weight to data packets with smaller numbers of hops or shorter geographic distances to their destinations reduce average delay significantly without any additional control packet exchange. The weighted-hop scheduling algorithm is used for modified AODV. Result show considerably smaller delay than the other scheduling algorithms. The reduction in the average delay decreases as the mobility of nodes.

TABLE 1 : AVERAGE QUEUE LENGTH ACROSS ALL NODES

Number of Sources	Pause Time (s)	Average Queue Length (packets)		
		Min	*Median*	*Max*
10	0 900	0.52 050	0.55 0.50	0.65 4.21
20	0 900	0.56 0.50	0.97 0.51	6.35 0.58
30	0 900	1.42 0.50	9.00 0.69	18.23 52.61
40	0 900	1.90 0.51	14.0 0.94	34.26 58.39

TABLE II. : SIMULATION PARAMETER

Parameter	Value
Transmission range	100m
Topology size	300x300m
Simulation time	900s
Packet size	512bytes
Packet rate	4pkt/s
Data sessions	5,10, …,35 (Seconds)
Traffic type	CBR/UDP
Routing protocol	AODV
Number of Nodes	20,30,..,100
Number of runs	10
Antenna type	Omni Antenna
MAC protocol	IEEE 802.11
Maximum speed	2,5,7,10 m/s

6. CONCLUSION

Authentication is one of the security metrics considered to improve security in AODV and DSR. In this thesis, Dual Hash authentication technique is applied to AODV protocol. Here the public one way hash function is used to authenticate the RREQ twice so that the routing packets include not only the RREQ but also two hash values (H1, H2) where H2 is used to check whether the received routing packet has been modified and H1 is used to prevent the current node modifying the packet. AODV with DHT implementation improves the packet delivery ratio by a margin of 7%. It reduces the Packet Loss by a margin of 3% and 11% and increases the control overhead by a margin of 19% and 26% when the mobility of nodes is 10 m/s and 20 m/s respectively. In addition to this, SHORT, an optimized routing technique is applied to minimize the delay caused by the application of Dual Hash Technique. Applying SHORT to DHT in AODV further improves Packet Delivery Ratio and reduces Packet Loss.

The same Dual Hash Technique is applied to DSR protocol. Here the performance of the DSR protocol is analyzed by applying Dual Hash authentication technique with SHORT. The results have shown that DSR has performed slightly better in the case of control overhead and Packet Loss when compared to AODV. AODV has performed better in the case of Packet Delivery Ratio when compared to DSR.

7. FUTURE SCOPES

This work has been carried out currently on the reactive routing protocols AODV and DSR. In future, these security mechanisms may be tried along with some traditional shortest path algorithms using the above routing protocols. The performance of these authentication mechanisms and intrusion detection systems may be tried with other reactive and proactive routing protocols. The parameters other than those considered in this work such as end-to-end delay and communication overhead may be taken into account in the future. Moreover, other security mechanisms like RSA algorithm, Elliptic curve cryptography may also be applied in the reactive routing protocols AODV and DSR and their performance can be analysed.

REFERENCES

[I] Asad Amir Pirzada, Chris McDonald, and Amitava Datta, Member, IEEE "Performance Comparison of Trust-Based Reactive Routing Protocols"IEEE Transaction On Mobile Computing, vol. 5, no. 6, June 2006.

[2] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of cooperative blckhole attack in MANET", Journel of networks, vol. 3, no. 5, pp. 13-20, May 2008.

[3] S. Deswal and S. Singh, "Implementation of Routing Security Aspect in AODV", IntI. Journal of computer Theory and Engineering. Vol 2, No.1 Feb 2010.

[4] Pramod kumar Singh, Govind Sharma "An Efficient Prevention of Black Hole problem in AODV Routing Protocol in MANET", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[5] Morli Pandya, Ashish kr. Shrivastava, Rajiv Gandhi Proudyogiki Vishwavidyalaya "Improvising the Performance

with Security of AODV Routing Protocol in MANETs" 2013 Nirma University International Conference on Engineering.

[6] Seryvuth Tan, Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs" , 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing.

[7] Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathurl and Prashant Khurana, "A Modified AODV against single and collaborative Black Hole attacks in MANETs", 2013 27th International Conference on Advanced Information Networking and Applications Workshops.

[8] Mehran Abolhasan, Tadeusz Wysocki, and Eryk utkiewicz, **"**A review of routing protocols for mobile ad hoc networks", Ad Hoc Networks, Volume 2-1 (2004), pp: 1-22.

[9] Dhirendra Kumar Sharma, Sanjay Kumar Biswash and Chiranjeev Kumar, "Enhancement of Split Multipath Routing Protocol in MANET", International Journal of Computer Science and Engineering, Volume: 02, No: 3, (2010), pp: 679-685.

AUTHOR'S PROFILE

Navneet Kumar has received his Bachelor of Engineering degree in Computer Science and Engineering from Millennium Institute of Technology and Science, Bhopal (India) in the year 2013. At present he is pursuing M.Tech. With the specialization of Computer Science and Engineering in Millennium Institute of Technology and Science, Bhopal (India). His area of interest is Computer networking, Cloud Computing, and Java.

Prof. S. R. Yadav has received his Bachelor of Engineering in Computer Science and Engineering from G.I.E.T. Gunupur under B.U. Orissa in the year 2006. M.Tech. in Computer Science and Engineering from P.G. Department of Computer Science Engineering under B.U. Berhampur, Orissa in the year 2009. M.B.A. in HR from Academy of Management Bhopal under B.U. Bhopal, M.P. in the year 2014.He is a Ph.D. Scholar of Computer science and engineering PAHER Univ. Udaipur, Rajasthan, India. At present he is working as an Associate Professor at Millennium Institute of Technology and Science, Bhopal.(India). His areas of interests are Data Mining, Intrusion Detection System using Data Mining and Neural Networks.