ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Performance Evaluation of Secured AODV v/s Impersonated AODV

Payal Gupta*
M.Tech Scholar, Deptt. Of CSE,
Jind Institute of Engg. & Technology
Jind(Haryana),India
payal_15gupta@yahoo.com

Kuldeep Singh
Assistant Professor, Deptt. Of CSE,
Jind Institute of Engg. & Technology
Jind(Haryana),India
kuldeep_cdlu@yahoo.co.in

Abstract: An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. Due to Open Medium, dynamic topology, Distributed Cooperation, Constrained Capabilities ad hoc networks are vulnerable to many types of security attacks. This paper is about the prevention of impersonation Attack. The proposed system is based on authentication system. In which cryptographic signature matching is performed between the mobile station and the base station. we have used Diffie-Hellman based cryptography approach to perform the secure transmission over the network. The system is implemented in ns2 with AODV protocol and analysis is presented using Xgraph.

Keywords: MANET, AODV, Security, Impersonation attack,NS2

I. INTRODUCTION

Wireless networks have become increasingly popular in the computing and communication industries, since their emergence in the '70s. This is predominantly true within the past decade, which has seen wireless networks evolve with the purpose of enabling better mobility. There are two variations of mobile wireless networks [1] - the first is known as *infrastructure* network, i.e., a network with fixed and wired gateways and the second is *infrastructure-less* mobile network, better known as an *ad hoc network*. Wireless mobile ad hoc networks have no fixed routers; hence, all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Meanwhile, nodes of these networks function as routers which discover and maintain routes to other nodes in the network [2].

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless [3]. It is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently; each must forward traffic unrelated to its own use, and therefore be a router. The network topology may change with time as the nodes move or adjust their transmission and reception parameters[4].Thus, a MANET has several salient characteristics: dynamic topologies, resource constraints, limited physical security and no infrastructure.

Possible applications of MANET include[5]: Soldiers relaying information for situational awareness on the battlefield, business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference; and emergency disaster relief personnel coordinating efforts after a fire, hurricane, or earthquake.

Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology.

a. ***Reactive protocols*** - Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded [6,7]. When a node wants to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. Examples of this class include DSR, AODV and ABR.

b. ***Proactive protocols*** - Proactive routing protocols work as the other way around as compared to reactive routing protocols. These protocols constantly maintain the updated topology of the network. Every node in the network knows about the other node in advance, in other words the whole network is known to all the nodes making that network. All the routing information is usually kept in tables [8]. Whenever there is a change in the network topology, these tables are updated according to the change. The nodes exchange topology information with each other; they can have route information any time when they needed [8]. Examples of this class include DSDV, WRP.

c. ***Hybrid protocols*** - Hybrid protocols exploit the strengths of both reactive and proactive protocols, and combine them together to get better results. Hybrid protocols divide the network into areas called zones which could be overlapping or non-overlapping depending on the zone creation and management algorithm employed by a particular hybrid protocol. The proactive routing protocol operates inside the zones, and is responsible for establishing and maintaining routes to the destinations located within the zones. On the other hand, the reactive protocol is responsible for establishing and maintaining routes to destinations that are located outside the zones. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. [9].

II. AODV ROUTING PROTOCOL

We use one of the reactive protocol i.e. AODV for the implementation of the impersonation attack.

AODV [11] is a distance vector routing algorithm which discovers route whenever it is needed via a route discovery process. AODV possesses a significant feature that once the algorithm computes and establishes the route between source and destination, it does not require any overhead information with the data packets during routing. Moreover the route discovery process is initiated only when there is a free/available route to the destination.Route maintenance is also carried out to remove stale/unused routes. The algorithm has the ability to provide services to unicast, multicast and broadcast communication. AODV routing algorithm has two phases i.e. Route Discovery and Route Maintenance. The AODV routing protocol is a reactive routing protocol; therefore, routes are determined only when needed.

When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP)[11]. The RREP is unicast in a hop by hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table. If data owns and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop by hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary.Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected.

In general, any wireless network is highly vulnerable to security attacks due to their Limited Bandwidth, Dynamic Topology, No Centralized Control, Limited Battery Power and dealing with this is one of the main challenges of developers of these networks today. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. The different attacks can be classified based on their nature as either passive or active attacks [10]. A passive attack attempts to illegitimately acquire valuable information by listening to the traffic without disrupting the operation of the routing protocol. Hence detection of passive attacks is highly difficult. On the other hand, active attacks alter the flow of data either by inserting false packets or by modifying the packet contents. Active attacks can further be classified into Internal and External attacks. Internal attacks are caused by a node that belongs to the same network as the victim, whereas external attacks are caused by nodes that do not belong to that network.

We consider the impersonation attack in this paper and try to mitigate its effect on MANET.

III. IMPERSONATION ATTACK

Impersonation attack are also called *spoofing* attacks.This attack occurs when one entity assumes the identity of another node in the network and receives messages on behalf of this node. Through this way, the attacker can gain the access to confidential information [10]. The attacker reads & can modifies the messages between the two nodes without letting them know about this as shown in fig.1 [12].

This is the first step for most attackers to introduce more sophisticated attacks to the network. The attacker may even be able to reconfigure the network as a super user who has special privileges so that more attackers can join the network and disrupt the operation of network. A malicious node propagate

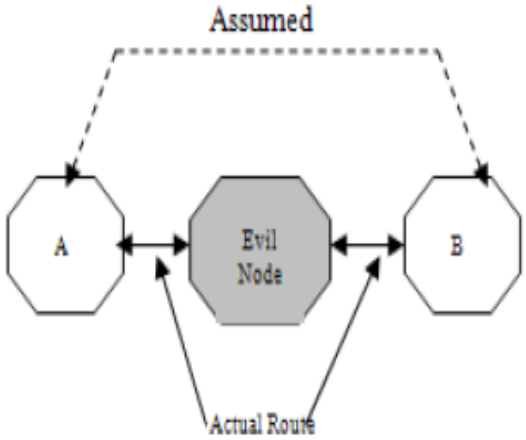

Figure1: Impersonation Attack

Fake routing information in the network to obstruct proper routing[13]. A compromised node may also have access to encryption keys and authentication information. Some of the impersonation attacks include:

a. ***Man-in-the-Middle Attack:*** In this attack, a malicious node impersonates the receiver with respect to the sender, and the sender with respect to the receiver, without having either of them realize that they have been attacked with an intension to read or modify the messages between two parties [14].

b. ***Sybil Attack:*** In the Sybil attack [15], an attacker pretends to have multiple identities. A malicious node can behaves as if it were a larger number of nodes either by impersonating other nodes or simply by claiming false identities. Sybil attacks are classified into three categories: direct/indirect communication, fabricated/stolen identity, and simultaneity. In the direct communication, Sybil nodes communicate directly with legitimate nodes, whereas in the indirect communication messages sent to Sybil nodes are routed through malicious nodes. An attacker can fabricate a new identity or it can simply steal it after destroying or temporarily disabling the impersonated node. All Sybil identities can participate simultaneously in the network or they may be cycled through.

IV. RELATED WORK

The following papers shows the relative work carried out for impersonation attacks in MANETS and possible solutions given.

Bing Wu et al. [5] proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN, every node that forwards a route discovery or a route reply message must also sign it, (which is very computing power consuming and causes the size of the routing messages to increase at each hop).

Radha Sankararajan et al. [16] proposed the algorithm that can prevent and also eliminate multiple attacks simultaneously, called MIST algorithm (Modification, Impersonation, Sleep deprivation and TTL attacks). This algorithm is written on Node Transition Probability (NTP) based protocol which provides maximum utilization of bandwidth during heavy traffic with less overhead.

Thorsten Holz et al.[17] used different kinds of techniques that can be helpful in eliminating Impersonation attacks , for example multi-factor authentication, biometrics, or special hardware or software. While techniques like SpoofGuard , Dynamic Security Skins , or Transport Login Protocol can protect against certain forms of impersonation attacks, e.g., classical phishing attacks, they can not stop keylogger-based attacks.

Michel Barbeau et al. [18] considered two defense strategies1) Radio Frequency Fingerprinting, and 2) User Mobility Profiling that look promising in providing defenses against impersonation attacks.

A. Radhika et al. [19] proposed Mobile Agent based algorithms or Ant Routing algorithms which is a class of swarm intelligence and try to map the solution capability of ant colonies for routing in Manets.

Latha Tamilselvan and Dr. V. Sankaranarayanan [10] proposed Secure Ad hoc On-Demand Distance Vector (SAODV) which is an extension of the AODV routing protocol that can be used to prevent Impersonation attack in mobile ad hoc network (MANET).

V. DETECTION OF IMPERSONATION ATTACK

The below diagram describes the detection system flow indicating inputs, internal information flow and output. Bear in mind that the thread work concurrently and the flow demonstrate only the logical path of the information through the system.

System internal flow consists of the following stages:

a. Collector daemons constantly collect incoming statistics. Periodically the collector threads query the daemons for the current statistics.
b. The sampled statistics received by the collector threads are committed to the database, normalized by time.
c. The post collector periodically samples the database for raw statistics samples and estimates the probability for common events such as spoofed traffic or changes in traffic behavior such as changes in packet size, TCP/UDP destination ports distribution and etc.
d. The post collector commits the estimations in the database.
e. The analyzers periodically sample the database for estimations and raw statistics and evaluate the probability for an attack
f. Attack evaluation are written to log files or printed to the screen upon user request.

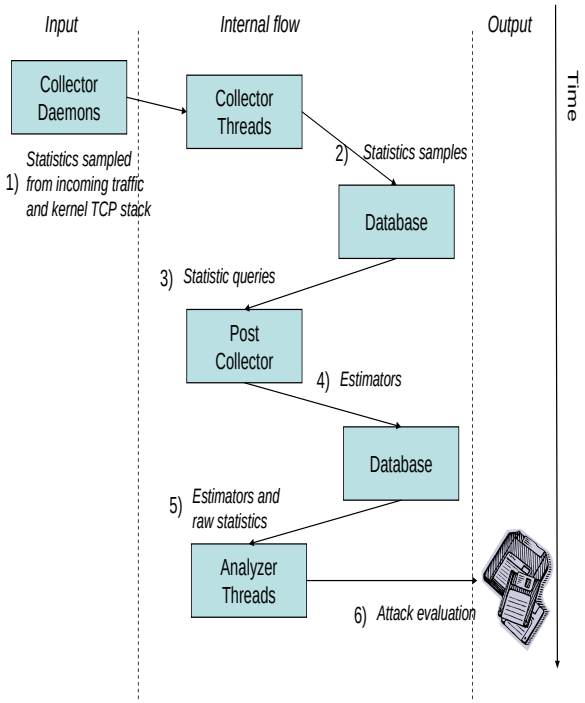

Figure 2: Detection System flow Diagram

VI. METHODOLOGY

The proposed work is about detection of Impersonation attack between the communication taken place between the source and the destination. In this work, an authentication system is presented here to detect and resolve the problem of Impersonation attack. In this work each node is defined as an intelligent node that having the cryptographic algorithm implementation on it. As a node start has to start the communication it generates the neighbor nodes list and find the nearest neighbor. It generates a “hello” message and encrypt it by using the public key of the neighboring node, After the encryption it pass the message to the neighboring nodes. As the neighboring node receives the message it will perform the decryption using its own private key and then send the acknowledgement to the sender node back. If the neighbor node is not authenticated it will remove its entry from the routing table and continue its work after updation of cache table. Immediate to this it will transfer data to its most eligible next node. To check the eligibility of authenticated node it will also observe some other factors like load on the node, response time etc. As the node reply it check if the response time is greater then its estimated response time then it will again exclude that particular node from the list. There also exist some diagnostic algorithm to transfer the data with true decision making. The complete process is repeated node by node till the destination node is not achieved.

Here the exact algorithm is presented

ALGORITHM

Impersonation (S,D)

[S is the source node and D represents the Destination Node over the network]

{

a) Find the path between S and D called P1,P2,P3….Pn
b) For Each Node Generate the KeyGroup for the communication using Deffie-Hellman Algorithm
    a. Unique Priavate Key Pvk
    b. Global Public Key Puk
    c. Shared Key Shk
c) On Node S Retrive the Public Key of D and Perform the encryption
d) Perform the Communication between Source and Destination
e) For Each Node in path called Pi verify the shared key
f) On Receiver Side Perform the Decoding using PrivateKey(D)
g) Discard the Bad Packets coming from unauthorized nodes.
h) Perform the Secure Communication over the network.

}

VII. RESULTS

In this section, we choose ns-2 simulator as platform to implement reactive protocol and conduct simulations.

A. Simulation Environments:

Here the basic parameters of the proposed work are presented in Table 1 respective to the simulation environment. The system is implemented on NS2 simulator and XGraph is used as the tool for graph analysis.

Table 1: parameters used in simulation

Parameter	Value
Number of Nodes	50
Topography Dimension	500m*500m
Traffic Type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11MAC Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni Directional
Protocol	AODV

The mobile adhoc network comprising of 50 mobile nodes is constructed in the NS-2 simulator with the use of TCL script in the topological boundary area of 500 m x500 m. The position of the mobile nodes is defined in terms of X and Y coordinates values and it is written in the movement scenario file.

A NS2 application will be used to generate sample data. . To test the performance of all of the above stated approaches, a program is written in tcl and tested in real environment.

B. Performance Metrics:

We have considered the following network parameters for evaluating the performance of the proposed approach.

a) Packet loss - Packet loss is the difference between the packets sent and the packets received. Packet loss for malicious node is counted by how many of the packets is there which could not reach to the destination node and are absorbed by the impersonated attacker.

b) Packet Delay - Packet delay is the average delay between the sending of the data packets by the CBR sources and its receipt at the corresponding CBR receiver. This consists of the delays caused by the buffering and processing at the intermediate nodes at the MAC layer.

c) Packet Transmission - The number of packets sent by the source and received at the Destination.

d) Byte Transmitted - A byte is a sequence of eight bits. In computer networking, some network protocols send and receive data in the form of byte sequences. Bytes are used not only in networking, but also for computer disks, memory, and central processing units (CPUs). Generally, bytes are measured in bits per sec (bps).

e) Bitrate - In telecommunications and computing, bit rate (sometimes written bitrate , data rate) is the number of bits that are conveyed or processed per unit of time. Bitrate, as the name implies, describes the rate at which bits are transferred from one location to another.

f) Packet Loss Rate – The rate at which the packet is lost during communication from source to destination.

C. Analysis Results:

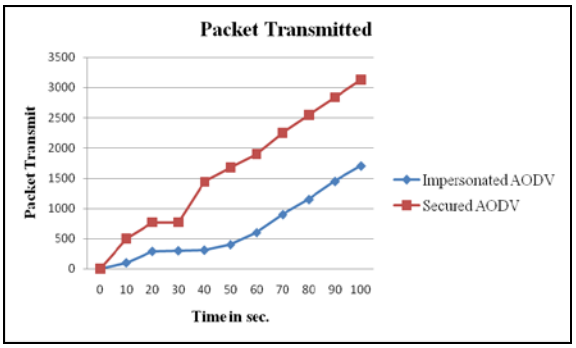

Figure 3: Graph of Comparison Results for Packet Transmitted

Here figure 3 is showing the comparative analysis of packet transmitted over the network. As we can see after implementing the proposed approach the secured AODV transmits more packets over the network as compared to impersonated AODV. The Table 2 shows the two comparison values between impersonated AODV & secured AODV for packet transmitted parameter.

Table 2: Packet Transmitted values

Packet Transmitted		
Time in sec.	**Impersonated AODV**	**Secured AODV**
0	0	0
10	100	500
20	290	770
30	300	770
40	310	1440
50	400	1680
60	600	1900
70	900	2250
80	1150	2550
90	1450	2840
100	1706	3134

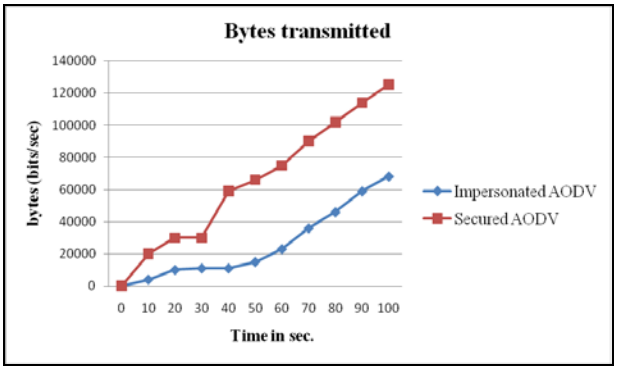

Figure 4: Graph of Comparison Results for Bytes Transmitted

Here figure 4 is showing the comparative analysis of bytes transmitted over the network. As we can see after implementing the proposed approach the bytes transmitted for Secured AODV is higher than Impersonated AODV over the network. The Table 3 shows the two comparison values between impersonated AODV & secured AODV for bytes transmitted parameter with respect to time.

Table 3: Bytes Transmitted Values in bps

Bytes Transmitted		
Time in sec.	**Impersonated AODV**	**Secured AODV**
0	0	0
10	4000	20000
20	10000	30000
30	11000	30000
40	11000	59000
50	15000	66000
60	23000	75000
70	36000	90000
80	46000	10200
90	59000	11400
100	68240	12536

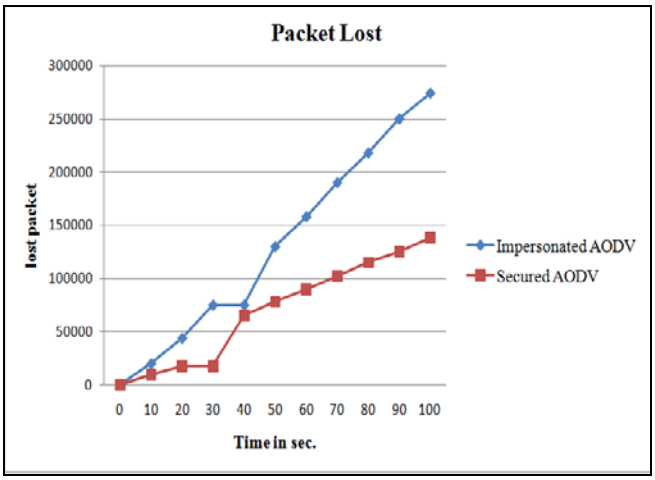

Figure 5: Graph of Comparison Results for Packet Lost

Here figure 5 is showing the comparative analysis of packet lost over the network. As we can see after implementing the proposed approach the packet loss over the network is decreased nearby 50% for secured AODV as compared to impersonated AODV. The Table 4 shows the two comparison values between impersonated AODV & secured AODV for Packet lost parameter with respect to time.

Table 4: Comparative values for Packet Lost

No. of lost packets		
Time in sec.	**Impersonated AODV**	**Secured AODV**
0	0	0
10	20000	10000
20	44000	18000
30	75000	18000
40	75000	65000
50	130000	78000
60	158000	90000
70	190000	102000
80	218000	115000
90	250000	125000
100	274090	138323

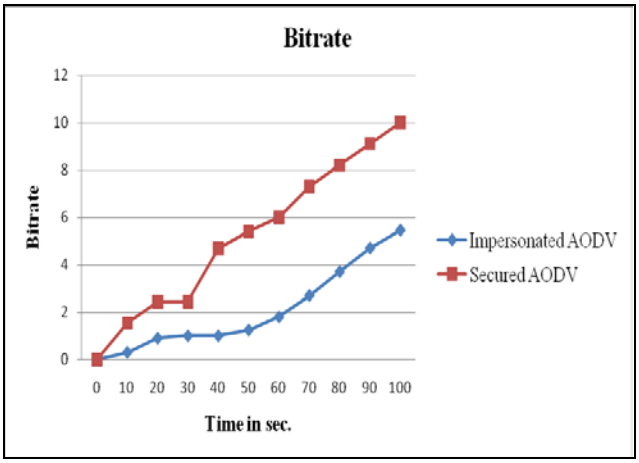

Figure 6: Graph of Comparison Results for Bitrate

Here figure 6 is showing the comparative analysis of bitrate over the network. As we can see after implementing the proposed approach the bitrate over the network is increased. The Table 5 shows the two comparison values between impersonated AODV & secured AODV for Bitrate parameter with respect to time.

Table 5: Comparative values for Bitrate

Bitrate		
Time in sec.	**Impersonated AODV**	**Secured AODV**
0	0	0
10	0.3	1.55
20	0.9	2.45
30	1	2.45
40	1	4.7
50	1.25	5.4
60	1.8	6
70	2.7	7.3
80	3.7	8.2
90	4.7	9.1
100	5.45	10

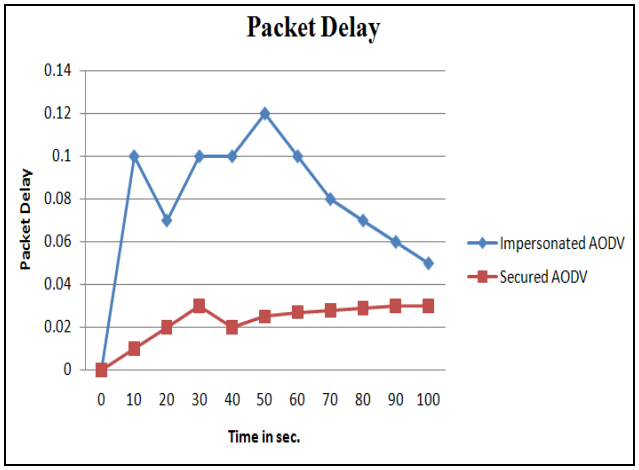

Figure 7: Graph of Comparison Results for Packet Delay

Here figure 7 is showing the comparative analysis of Packet Delay over the network. As we can see after implementing the proposed approach there is nearly 40% decrease in the Packet Delay. The Table 6 shows the two comparison values between impersonated AODV & secured AODV for Packet Delay parameter with respect to time.

Table 6: Comparative values for Packet Delay

Packet Delay		
Time in sec.	**Impersonated AODV**	**Secured AODV**
0	0	0
10	0.1	0.01
20	0.07	0.02
30	0.1	0.03
40	0.1	0.02
50	0.12	0.025
60	0.1	0.027
70	0.08	0.028
80	0.07	0.029
90	0.06	0.03
100	0.05	0.03

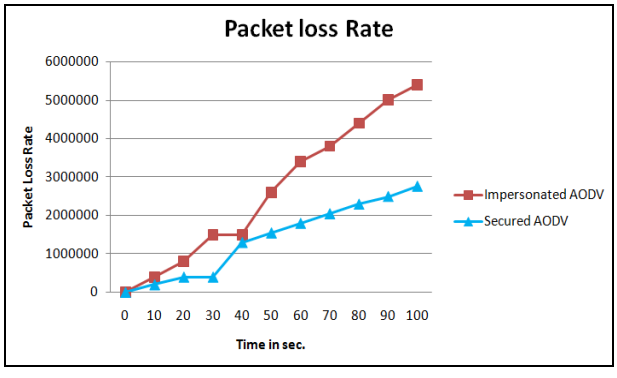

Figure 8: Graph of Comparison Results for Packet Loss Rate

Here figure 8 is showing the comparative analysis of Packet Loss rate over the network. As we can see after implementing the proposed approach the Packet Loss rate decreased by 50% over the network. The Table 7 shows the two comparison values between impersonated AODV & secured AODV for Packet Loss Rate parameter with respect to time.

Table 7: Comparative values for Packet Loss Rate

Packet Loss Rate		
Time in sec.	**Impersonated AODV**	**Secured AODV**
0	0	0
10	400000	200000
20	800000	400000
30	1500000	400000
40	1500000	1300000
50	2600000	1550000
60	3400000	1800000
70	3800000	2050000
80	4400000	2300000
90	5000000	2500000
100	5400000	2766460

VIII. CONCLUSION & FUTURE WORK

The proposed work is about the prevention of Impersonation Attack. In this present work we have used Diffie-Hellman based cryptography approach to perform the secure transmission over the network. The system is providing better throughput and less packet loss over the network. The system is implemented in a wireless network with AODV protocol. Here we have proposed a new algorithm for the above said task. The implementation is performed in ns2 and analysis is presented using Xgraph. The proposed system can be enhanced in future by other researchers like the work can be implemented on some specific network such as PAN, WiMax etc.

IX. REFERENCES

[1] E. M. Royer and T. Chai-Keong, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *Personal Communications, IEEE*, vol. 6, pp. 46-55, 1999.

[2] Mohamad Rizal Bin Abdul Rejab, "An Investigation Of TFRC Over MANET Routing Protocol", Universiti Ut Ara Malaysia, 2010.

[3] http://en.wikipedia.org/wiki/

[4] P. Padmanabhan, 1. Gruenwald, A. Vallur, and M. Atiquzzaman, "A Survey of Data Replication Techniques for Mobile Ad hoc Network Databases," *The VLDB Journal - The International Journal on Very Large Data Bases*, vol. 17, pp. 1143 - 1164,2008.

[5] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. °c 2006 Springer

[6] 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 Applictions, pp.90-100, Feb, 1999.

[7] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance

Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[8] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, 2003.

[9] http://www.netmeister.org/misc/zrp/zrp.html#SECTION00041000000000000000, last visited 12 Apr, 2010

[10] Latha Tamilselvan and Dr. V. Sankaranarayanan, "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007

[11] Vishal Pahal,* Amit Verma, Payal Gupta, "Classification of Routing Protocol in Mobile Ad Hoc Networks: A Review", IJCSET |November 2011 | Vol 1, Issue 10, 626-637

[12] Ankit Jain, Arnika Jain, Pramod Kumar Sagar" Various Security Attacks and Trust Based Security Architecture for MANET"GJCST,Nov2010

[13] Abari Bhattacharya, Prof. Himadri Nath Saha "A Study of Secure Routing in MANET: *various attacks and their Countermeasures"*Kolkata ,India

[14] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.),Springer, 2008.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004

[16] Edna Elizabeth Nallathambi, Radha Sankararajan, Vaithiyanathan Sundaram and Gracelin Sheeba "A Secure Routing Protocol to Eliminate Integrity, Authentication and Sleep Deprivation Based Threats in Mobile Ad hoc Network" Journal of Computer Science 7 (6): 924-936, 2011 ISSN 1549-3636© 2011 Science Publications

[17] Thorsten Holz,Markus Engelberth,Felix Freiling "Learning More About the Underground Economy:A Case-Study of Keyloggers and Dropzones" University of Mannheim Laboratory for Dependable System December 18, 2008

[18] Michel Barbeau1, Jyanthi Hall1, and Evangelos Kranakis, "Detecting Impersonation Attacks in Future Wireless and Mobile Networks" School of Computer Science, Carleton University, Ottawa, K1S 5B6, Canada

[19] A. Radhika, D. Kavitha, Dr. D. Haritha "MOBILE AGENT BASED ROUTING in MANETS – ATTACKS & DEFENCES"Network Protocols and Algorithms ISSN 1943-3581 2011, Vol. 3, No. 4

