Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Modifications of AODV Routing Protocol to Prevent the Effects of Blackhole Attack in MANET

Mulugeta Adibaru[1]
College of Engineering & Technology
Wollega University
P o s t B o x No: 395
Nekemte, Ethiopia

Ramesh Babu P[2]
College of Engineering &Technology
Wollega University
P o s t B o x No: 395
Nekemte, Ethiopia

Md Asdaque Hussien[3]
E I T - Mekelle
Mekelle University
P o s t B o x No: 231
Mekelle, Ethiopia

Abstract **- Mobile adhoc networks (MANETs) are composed of independent and self organized nodes without the need of any infrastructure. Mobile adhoc networks consist of mobile devices that are freely moving inside and outside in the network. These devices can operate as a host, a router or both at the same time. These nodes have the ability to organize themselves because of their self configurable capability; they can be organized immediately without the help of any infrastructure. Due to various features like open medium, dynamic topology, lack of defensive mechanism, makes MANET more susceptible to security problems and attacks. Ad hoc On-Demand Distance vector routing protocol (AODV) is one of the best and most popular routing protocols in MANET. This routing protocol is frequently affected by well known black hole attack in which it injects a forged route reply message that considers as it has a fresh enough route to destination node. In this research we have modified AODV routing protocol to implement blackhole attack in NS-2 and measure its impact on the performance of AODV routing protocol by using different performance metrics like Average Throughput, Normalized Routing Overhead, Packet Delivery Ratio, and Number of Dropped Packets. After measuring the impacts of blackhole attack on the performance of normal AODV routing protocol we have implemented and simulated our proposed solution to prevent and minimize the effects of blackhole attack using NS-2. The proposed solution is implemented in NS-2 using AES symmetric cryptographic technique and digital signature schemes to secure AODV routing protocol of MANET from blackhole attack. After implementing and integrating our proposed solution in to NS-2, we have measured and analyzed the result of our proposed solution through NS-2 simulator with various network performance parameters. The simulation result shows that the proposed solution effectively prevents and minimizes the effects of blackhole attack in AODV routing protocol.**

Keywords: MANET, AODV, blackholeAODV, Digital Signature, Hash Function, AES.

I. INTRODUCTION

MANETs are independent and decentralized wireless systems [1]. It consist of mobile devices that are open in moving inside and outside in the network. Nodes are devices i.e. mobile phone, laptop, PDA, MP3 player and personal computer that are join in the network and are movable. These devices can operate as host/router or both at the same time. They can form random topologies based on their connectivity with each other in the network. These nodes have the ability to arrange themselves and because of their self configurable capability, they can be organized immediately without the need of any infrastructure. As adhoc networks are composed of independent and self managed nodes without any infrastructure, they are exposed to a lot of security threats and attacks [2]. One of these threats is the blackhole attack. In such types of attack, a malicious node absorbs all data packets in itself, in this way; all data packets in the network are dropped and captured by blackhole node. A blackhole node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery control messages of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination and to do this it sends RREQ packets to the neighbor nodes. Blackhole node does not use this process and in its place, they instantly respond to the source node with false information as though it has fresh enough route to the destination. Therefore source node uses this path and sends its data packets via the blackhole node to the destination assuming it is a true path. In any case, nodes in the network will regularly try to find a path for the destination, which creates the node consume its battery in addition to dropping packets. In this study, we simulated the blackhole attack in Mobile Adhoc Networks and evaluated its effect in the network. We also performed our simulations using NS-2 simulator software that consists of the number of all network protocols to simulate many of the existing network topologies. Tests are performed on different scenario to measure and compare the network performance with and without blackhole attack in the network. After that, we have proposed a solution to prevent the effects of blackhole attack in AODV routing protocol. This proposed solution is implemented in NS-2 using AES symmetric cryptographic technique and digital signature schemes to secure AODV routing protocols of MANET.

II. STATEMENTS OF THE PROBLEM

Security in mobile adhoc network is the most important fear for the basic functionality of wireless networks. Availability, confidentiality and integrity of data in wireless network can be considered to achieve the security issues of MANET. Some of the requirements to achieve secure communication between mobile nodes in MANET are:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

- A security association must be existed between mobile nodes to ensure authentication and non repudiation for trusted nodes.
- The confidentiality of mobile nodes must be preserved to exchange sensitive information between these nodes.
- Corrupted messages must be detected and blocked to maintain the integrity of exchanged messages within the network.

MANET mostly suffer from security threats because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear protection mechanism. In this research blackhole attack is concerned against AODV routing protocol.

III. MANETs Routing Protocol

Routing [3] is the process of moving information from a source to a destination in an internetwork. During the transfer of information at least one intermediate node within the internetwork is encountered. Mainly two activities are concerned in this concept: transferring the packets through an internetwork and determining optimal routing paths. The transferring of packets through an internetwork is known as packet switching which is straight forward, and the path determination could be very complex. MANET is the increasingly developing technology in the last 20 years [1]. Their attractiveness is also increased due to their dynamic nature, ease of deployment, and the no need of any infrastructure. MANETs summarize a new set of demands to be implemented and to provide well organized and better end to end communication. In MANET, there are different types of routing protocols each of them is applied according to the network situation [3].Thus routing protocols are classified into three different categories based on their functionality.

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

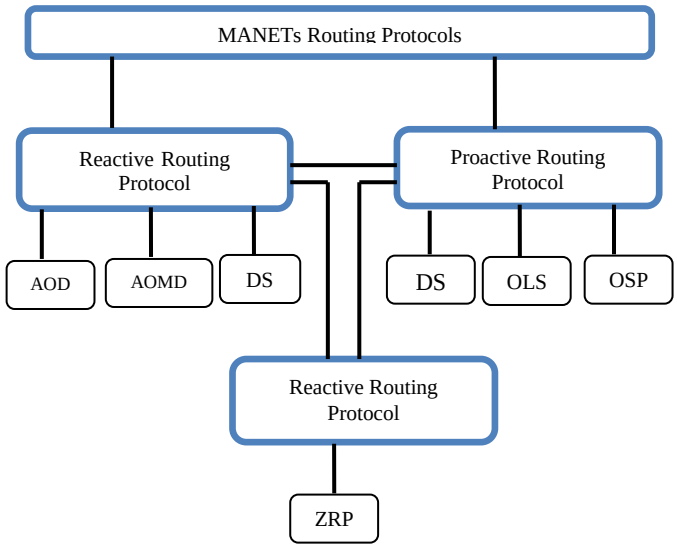


Figure-1: Classification of Routing Protocols

IV. Security Issues in Mobile Adhoc Network

Due to basic functionality mobile adhoc network Security is the most important concern [2] Confidentiality, availability of network services, and integrity of the data can be achieved by assuring that security issues have been met. Mobile Adhoc Networks often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. So battle field situation for the MANET against the security threats have changed due to these factors. Computer networks Security has been of serious concern which has widely been discussed and formulized in the last few years. Most of the discussions involved only static and networking based on wired systems. Nevertheless, mobile Adhoc networking is still in need of further discussions and development in terms of security [4]. With the emergence of ongoing and new approaches for networking, new problems and issues take places for the basics of routing. With the comparison of wired network Mobile Adhoc network is different. The routing protocols designed majorly for internet is different from the mobile Adhoc networks (MANET). Due to different factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks [5]. Major vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction and also open network medium. Despite of the above said protocols in Mobile adhoc network, there are attacks which can be categorized in Passive, Active, Internal, External and network layer attacks, Routing attacks and Packet forwarding attacks.

V. Blackhole attack in AODV

Blackhole attack is a type of denial of service where a blackhole node can draw all packets sent by the source node by falsely maintaining a fresh route to the destination and then attract without forwarding them to the destination [5]. In an adhoc network that uses the AODV routing protocol, a blackhole node imagined to have new and enough routes to all destinations requested by all the nodes and attracts the network traffic. When a source node transmits the route request (RREQ) message for the destination, the blackhole node instantly reacts with a route reply (RREP) message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a new and enough routes to the destination node. The source node assumes that the destination is at the back of the blackhole node and then discards all the other RREP packets coming from other intermediate nodes. The source node then starts to send its data packets to the destination through the blackhole node by trusting that these packets will deliver to the destination.

In figure-2, assume node B is a blackhole node. When source node S broadcasts a RREQ packet to the entire neighbor node towards the destination node D, nodes A, B and C receive it. Node B, being a blackhole node, this node immediately sends back a RREP packet with highest sequence number before any other node responds, even if any intermediate node sends

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

RREP to the source node S without checking up its routing table for the requested route to the destination node D argue that it has fresh enough route to the destination. Node S receives the RREP from B further on the RREP from A and C. Hence, source node S updates its routing table for the new route to the particular destination node discards replies from node A and C even from an actual destination node D and assumes that the route through node B is the shortest and fresh path to reach the destination. Once a source node S saves a route, it starts to sends the data packets to the destination node D through this path. So, node B drops all the packets coming from source node S which produce blackhole problem rather than forwarding them to the destination node D.

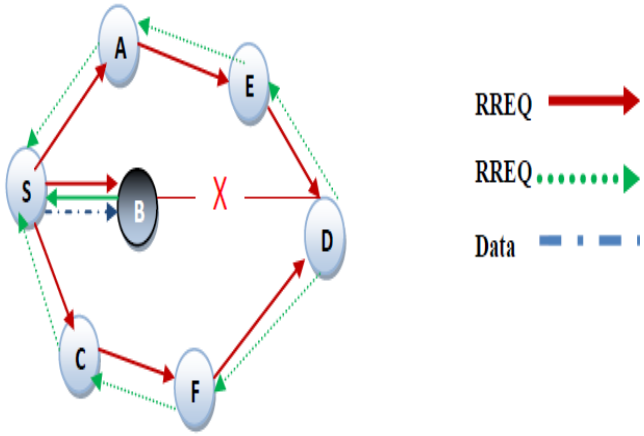


Figure-2: illustration of blackhole attack

VI. METHODOLOGY AND ALGORITHM OF THE PROPOSED WORK

Mobile ad-hoc network is wireless network that contains a collection of different nodes communicate with each other without having to set up any infrastructure. But the security of such network is a major issue. So to achieve secure communication in these types of network some requirements must be fulfilled [6]:-

- Between mobile nodes, a security association must be existed in the network; these security associations ensure non repudiation and authentication of trusted nodes.
- Between the nodes in the network, sensitive information must be exchanged confidentially.
- Integrity of the information exchanged within the network has to be maintained so that corrupted messages are detected and blocked.

In this research, we are used symmetric cryptographic algorithms, to preserve integrity and confidentiality of information exchanged between mobile nodes and digital signature and hash function to ensure the authentication and integrity of trusted nodes in AODV routing protocol to prevent the effects of blackhole attack in MANET. Symmetric cryptographic algorithm enables us to store the data in a condensed or compressed encryption form which results in a small size file that means, it improves the performance of MANET. Also it provides faster encryption/ decryption Algorithm. Due to these Advantages we have used Advanced Encryption Standard (AES), which is one of the favorite and currently used types of symmetric cipher algorithm, to perform data encryption and decryption.

A.Digital Signature

It is used to authenticate the identity of the sender of the message. It also guarantees that the original contents of the message have not been altered. If the public key of the source node is known, any node can be verified the digital signature. This makes digital signature is scalable to large numbers of receiver nodes. In order to protect the integrity of the immutable data in RREQ and RREP messages we use Digital signature algorithm. When a node receives a RREQ, it first verifies the signature before creating or updating a reverse route. Only if the signature is verified, it stores the route. Otherwise, RREQ is rebroadcasted. When a RREQ is received by the destination itself, it will reply with a RREP only if the AODV's requirements are satisfied. This RREP will be sent to the source node along with digital signature. When RREP, it first verifies the signature before creating or updating a route. Only if the signature is verified, it stores the route which is received by the node the signature of the RREP.

B.Hash Function

A Cryptography hash function is considered as a function because it takes an input message and produces an output. It takes a message of arbitrary length that can be transformed in to a string of bits and computes from it a fixed-length or short number. The Cryptographic hash value, such that any intentional or unintentional modification to the data with very high possibility will modify the hash value. The data that has to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digests.

In hash function the hash of a message y, represented as h (y) has the following properties [9]:

- ✓ For any message y, it is relatively easy to compute h (y). This means that in order to be practical it can't take a lot of processing time to compute the hash.
- ✓ Given h(y), there is no way to find an y that hashes to h(y) in a way that is substantially easier than going through all possible values of y and computing h(y) for each one.
- ✓ Even though it is clear that many different values of y will be transformed to the same value h (y) because there are many more possible values of y, it is computationally in-feasible to find two values that hash to the same thing.

Hash chain algorithms can be used to improve the effectiveness of public key algorithms. The best known public key algorithms are sufficiently processor intensive that it is desirable to compute a message digest of the message and sign that, rather than to sign the message directly. Because the message digest algorithms are

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

much less processor intensive, and the message digest is much shorter than the message. In our proposed solution we have used hash chain algorithm to authenticate the hop count field i.e. the only mutable fields of RREQ and RREP control messages, in such a way that allows every node that receives the message (either an intermediate node or the final destination node) to verify that the hop count has not been decremented by an attacker. Hash function avoids unauthorized modification of hop count by attacker nodes during the travel throughout the network. In our approach the middle node is allowed to response a route request packets (RREQ) and route reply packets (RREP) whenever the node has a fresh enough route to the destination nodes.

C. *The Proposed Algorithm*

In this section the detail algorithm of our proposed solution is presented.

Step-1: Source node wishes to send data packets to the destination

Step-2: Then Source checks its routing table if it has a current route to the destination

If (route is already existed)
{
Source node encrypts the data using AES then forwards to the destination using the path
Destination node receives and decrypts the data using AES
}
Else {

Step-3: Source creates route request (RREQ) and signs on immutable fields of this RREQ (IP
Address and Seq #) and apply hash function on mutable fields of RREQ (i.e. hop count)

Step-4: Then source broadcasts RREQ to neighbor nodes

Step-5: All Neighbor nodes received RREQ verify the signature and hash functions

If (not verified)
{
Intermediate node is blackhole node
This route is removed from the routing table after *active_route_timeout* interval
}
Else{

Step-6: Intermediate node compares the Destination Sequence # in its routing table and RREQ packet

If (not equal)
{
Intermediate node sets up a reverse entry for the source node.
Then after intermediate node rebroadcasts the RREQ to its neighbor
}
Else
{
The node is destination node.
The destination node prepares RREP and signing on immutable fields and hashing the
Mutable fields of it then sends back these packets to the source using reverse entry.
}
}

Step-7: The source node then verifies RREP containing digital signature and hash function on it

If (verified)
{
The path is authenticated and forward path entry is established
The source encrypts the data using AES cryptographic algorithm and sends it to the
destination using the forward path.
Destination node receives and decrypts the data using AES cryptographic algorithm.
}
Else
{
The path is not authenticated and the node is blackhole node
The route entry is deleted after active *route-time-out* interval and route is not longer
Valid and cannot be used again
Source finds the next route by broadcasting RREQ
}

VII. SIMULATION AND ANALYSIS OF RESULTS

In this part we present the performance evaluation of AODV routing protocol, the effects of blackhole attack on the performance of aodv routing protocol and our proposed Algorithm to prevent and minimize the effects of blackhole attack on AODV routing protocol using NS-2.

A.Simulation Parameters and Setup

For simulation and result analysis, we must require setting of simulation parameters and mobility models. The summarized simulation parameter is depicted in table 1.

Table -1: Simulation Parameters

Parameter	Value
Simulator	NS-2(Version 2.34)
Routing Protocol	AODV
Simulation Time	200 second
Number of Nodes	20,40
Traffic Model	Constant Bit rate(CBR)
Packet Size	512 bytes
Pause time	0,5,10,15,20
Maximum Speed	5 meter/second
Area	500m*500m
Packet Rate	4 packets/second
Number of black-hole nodes	5%,10%,15%20%,25%
Mobility Model	Random Way Point
MAC layer protocol	IEEE 802.11

In this research we have used Random Waypoint Model, where mobile node is allowed to move at random in any direction [10].Constant Bit Rate (CBR) traffic with a transmission rate of 8 packets per second is used. Nodes in our scenario select any arbitrary destination in the 500 X 500 M^2 area and moves with the speed of 5 meter per second. We

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

have used 20 and 40 node scenarios with change in pause times and number of blackhole nodes (in percent) with simulation times of 200 seconds to compare the performance of the protocols for low as well as high density environment and for low mobility of the nodes to high mobility.

B.Performance Evaluation Metrics

To asses and evaluate the performance of routing protocols various quantitative metrics are practiced. In our research study four different quantitative metrics have been used to evaluate the performance of AODV routing protocol with and without blackhole attack as well as our proposed solution. These selected performance metrics are described below.

Throughput

It is the measure of how fast we can actually send packets through network. The number of packets delivered to the receiver provides the throughput of the network. The throughput is defined as the total amount of data a receiver actually receives from the sender divided by the time it takes for receiver to get the last packet.

$$\text{Average Throughput} = \frac{\text{Number of Bytes Recevied} * 8}{\text{Simulation time} * 1000}\text{kbps}$$

Routing Overhead

It is the total number of control or routing (RTR) packets generated by routing protocol during the simulation. All packets sent or forwarded at network layer is consider as routing overhead.

$$\textbf{Routing Overhead} = \textbf{Number of RTR packets}$$

Packets Dropped

Some of the packets generated by the source will get dropped in the network due to high mobility of the nodes, congestion of the network etc.

$$\textbf{Dropped Packet} = \textbf{Sent Packet} - \textbf{Recvied Packet}$$

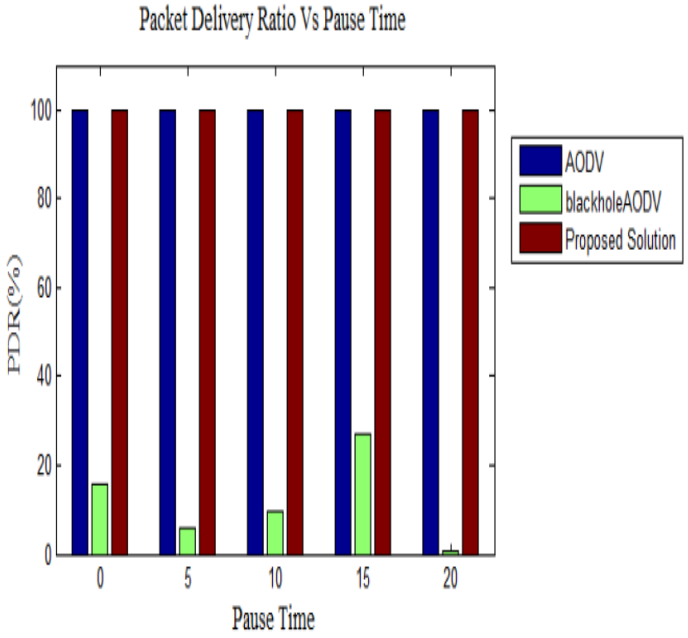
Packet Delivery Ratio

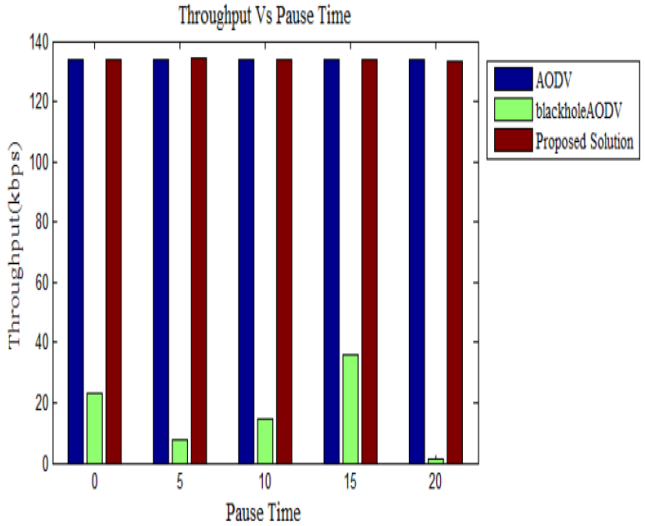
The ratio of the data packets delivered to the destinations to those generated by the CBR sources. It is the fraction of packets sent by the application that are received by the receivers.

$$\text{PDR (\%)} = \frac{\text{Number of Packets Recevied}}{\text{Number of Packets Sent}} * 100$$

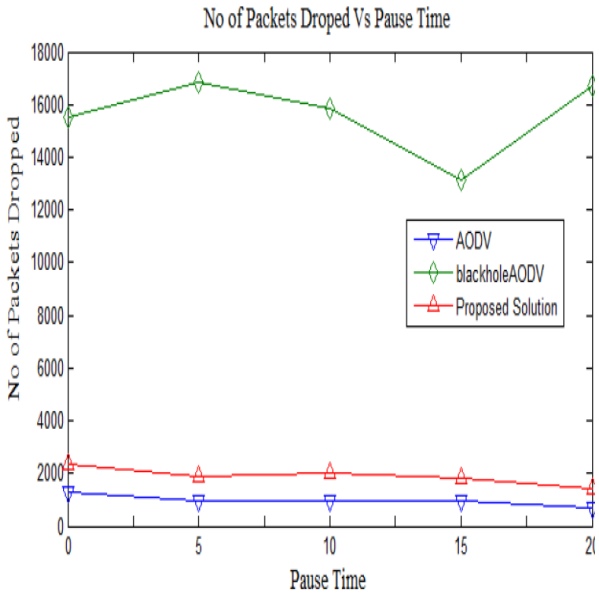
C. Simulation Results and Analysis

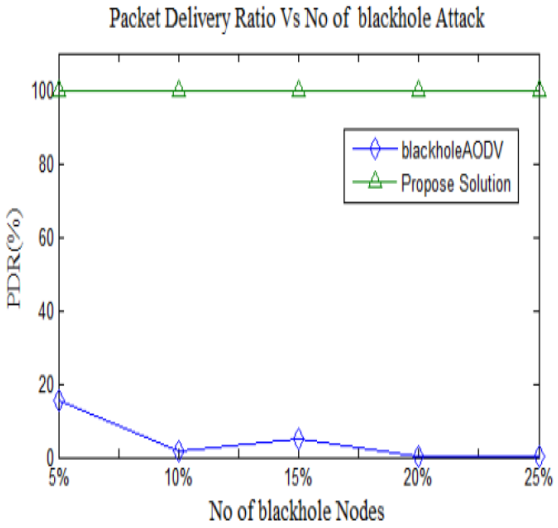
In this part we have measured the performance of AODV routing protocol with and without blackhole attack and its result is analyzed for both 20 and 40 node scenario with varying pause times of nodes from highest to lowest node mobility and with varying number of blackhole nodes to know the effects of blackhole nodes on the performance of AODV routing protocol. Then the performance of the proposed algorithm is measured and its result is analyzed with the same scenarios what we have performed on AODV routing protocol.

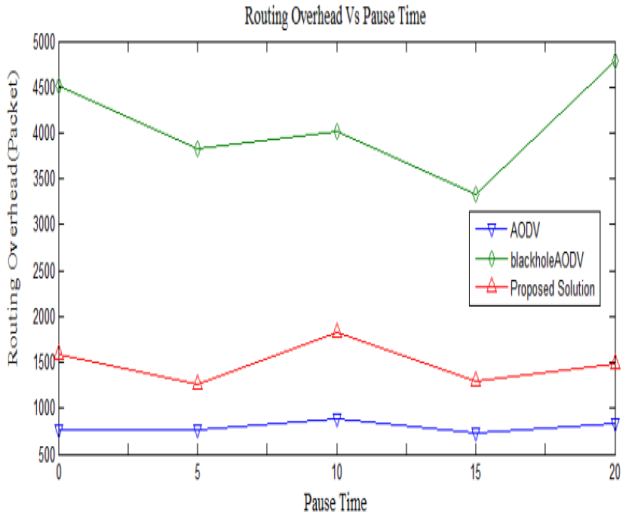


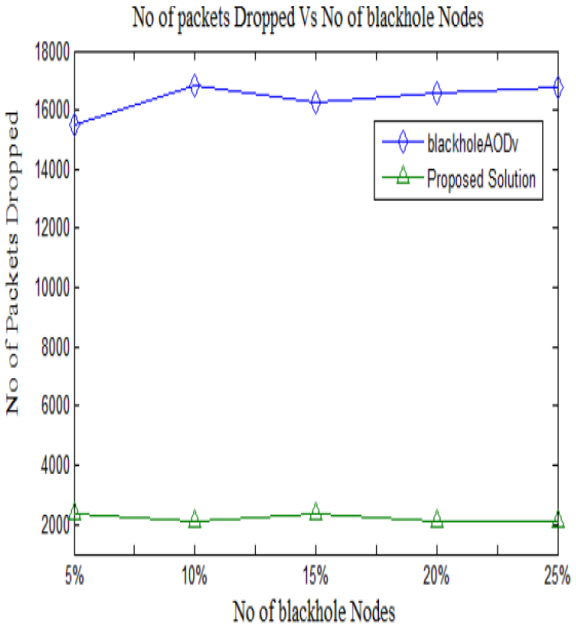


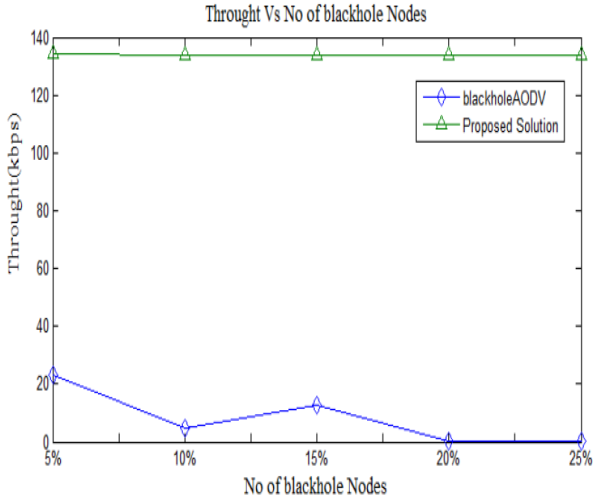
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

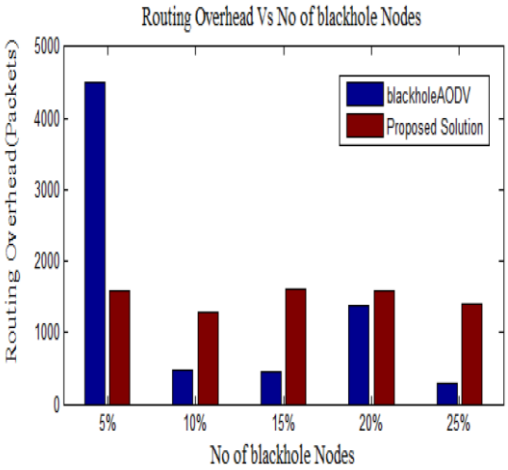












International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

VIII. CONCLUSION AND RECOMMENDATION

In this research, we have analyzed the effect of the blackhole attack in AODV routing protocol of MANET and proposed a solution for preventing the effects of this attack in an AODV routing protocol. For this purpose, we have implemented blackholeAODV that can behaved as blackhole nodes and its solution that can be used to prevent and minimized its effect in MANET. After we have implemented and simulated the blackhole attack in NS-2, we have seen the number of packets dropped and routing overhead of AODV routing protocol are increased but throughput and packet delivery ratio of this protocol are decreased in both 20 and 40 node Scenarios. That means its performance is decreased as the number of blackhole Nodes, pause time and number of nodes are increased in Mobile Adhoc Network. Commonly blackhole nodes or blackhole attack affects the overall network performance and connectivity of AODV routing of MANET. Finally, to prevent the effect of blackhole attack, we have implemented a solution by using AES Cryptography Algorithm and Digital Signature. As it can be observed from the simulation results, the proposed solution effectively prevents the effects of blackhole attack in AODV routing protocols of MANET. The throughput of AODV routing protocols at pause time zero in 20 and 40 nodes scenario are improved by 0.134% and 0.149% respectively. Hence, the performance of AODV routing protocol in terms of throughput is improved when the number of nodes are increased in the proposed solution. Also, the packet delivery ratio of this routing protocol is increased but routing overhead problems and numbers of packets dropped due to blackhole attacks are decreased in both 20 and 40 node scenarios of the proposed solution.

In this research we have implemented AODV routing protocol to behave as blackhole in NS2. To do this, we have used maximum sequence numbers and minimum hop count to study the behavior of blackhole attack. But, change in their strategy could be considered as a future work. For simulation, we have used throughput, packet delivery ratio, number of packets dropped and routing overhead performance evaluation parameters with change pause time and number of blackhole nodes. As a future work other parameters with change in their mobility, number of connection, speed of nodes etc could be tested. This proposed solution also can be tested for other routing protocols of MANET like DSR, DSDV, TORA and etc.

REFERENCES

[1]. Ullah and S. U. Rehman, "Analysis of Blackhole Attack on Manets Using Different Manet Routing Protocols," Master's Thesis, Bleking Institue of Technology, Sweden, June 2010.

[2]. P. Berwal, "Security issue in Manet:A Review," *International Journal of Engineering Sciences and Research Technology*, vol. 2, no. 12, pp. 3555-3557, Dec. 2013.

[3]. R. Kothari and D. Dembla, "Implementaion of Blackhole Security Attack Using Malicous Node For Enhanced DSR Routing Protocols Of MANET," *International Journal of Computer Applications(IJCA)*, vol. 64, no. 18, pp. 1-8, Feb. 2013.

[4]. K.Biswas and M. L. Ali. (2007, Mar.) Security Threats in Mobile Ad-hoc Network. Thesis.

[5]. S. Lu, L. Li, K.-y. Lam, and L. Jia, "SAODV: a MANET routing protocol that can withstand blackhole attack," in *Computational Intelligence and Security(CIS'09)*, vol. 2, 2009, pp. 421-425.

[6]. Suryawanshi and R. s. Tamhankar, "Performance Analysis and Minimization of Blackhole Attack in Manet," *International Journal of Engineering Research and Application(IJERA)*, vol. 2, no. 4, pp. 1430-1437, Jul. 2012.

[7]. A. Bhosle and Y. Pandey, "Applying Security to Data Using Symmetric Encryption in MANET," *International Journal of emerging Technology and Advanced Engineering*, vol. 3, no. 1, pp. 426-430, Jan. 2013.

[8]. B. Christian, "A Short Introduction to AES," University of Copenhagen Tutorial, October,2003.

[9]. William Stalling, *Cryptography and Network Security,principles and practice*, 5th ed. India: Pearson Education ,Prentice Hall, 2006.

C. bettstetter, "Stochastic Properties of The Random Waypoint Mobility Model: Epoch Time,Direction Distribution and cell change Rate," Technische Universitat Munchen,Institue of communication Networks , 2002.