International Journal of Electrical, Electronics and Computer Engineering **6**(2): 49-56(2017)

ISSN No. (Online): 2277-2626

Prevention and detection of Black hole attack in MANET using Cipher Security and Blocking the Black Hole Node

Prachi Pathak* and Mohd. Amjad Quaz**

**Research Scholar, Department of Electronics & Communication, SISTec, Bhopal, INDIA*
***Assistant Professor, Department of Electronics & Communication, SISTec, Bhopal, INDIA*

(Corresponding author: Prachi Pathak)

(Received 30 October, 2017 Accepted 15 November, 2017)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Security is the major concern in mobile ad hoc network (MANETs) due to its dynamic behavior. Mobile ad hoc network is the collection of nodes and it is infrastructure less network which means a node can join or leave in network simultaneously. Because of vibrant topology it is more susceptible to different kind of security attack such as Denial of service (DoS), wormhole, replay, masquerade, black hole etc. Such network uses routing protocol to transmit the packet from one end to another and each node behaves as host or router which can select suitable path for transmission of packet. In this, we determine the black hole attack in AODV routing protocol. Black hole is a network attack in which the malicious node advertises itself that it has freshest route to deliver the packet and then discard or drop it. This paper propose black hole attack detection using security algorithm and the simulation of this is perform on NS-2.34 network simulator.

Keywords: AODV, MANET, Black hole attack, Security threats, dynamic, Network Simulator

I. INTRODUCTION

Now a day mobility is becoming gradually important for users of computing systems. Science and technology has made it probably more influential, smaller and less expensive wireless communicating devices (nodes). As a consequence users gain flexibility and the capability to exchange information and sustain connectivity while roaming through a wide area. The mobile ad hoc networks (MANETs) are usually formed by a group of mobile nodes, interconnected via wireless links, which agree to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative. That means, if a node claims it can reach another node by a certain path or distance, the claim is trusted/true; similarly, if a node reports a link break, the link will no longer be used. While this assumption can fundamentally facilitate the design and implementation of routing protocols, it meanwhile introduces a vulnerability to several types of denial of service (DoS) attacks [1], particularly packet dropping attack. To launch such attack, a malicious node can stealthily drop some or all data or routing packets passing through it. Because of the lack of physical fortification and reliable medium access mechanism, packet dropping attack represents a severe threat to the routing function in MANETs. Anantagonist can effortlessly join the network and compromise a legitimate node then subsequently start dropping packets that are expected to be relayed in order to dislocate the regular communications. Subsequently, all the routes passing through this node fail to inaugurate a correct routing path among the source and destination nodes.

Mobile ad hoc network has foremost issues which are describing as follows [2]:

Infrastructure less: The primary challenge in Mobile adhoc networks is the infrastructure less environment so designing new network design is challenges.

Dynamic Environments: The other issue in the mobile ad-hoc networks is the dynamic environments means changing topology affect the communication of source to destination.

Power issue: The other issue in the MANET is the limited battery life and power so this reason it consumes lots of resources and increase the overhead.

Autonomous nature: Due to the absence of the admin there is no central coordinator to control the function of the mobile nodes due to this reasons the mobile nodes move in network and fails to configure that proper.

Device Discovery: When the new node comes in the network than this very important to update their existence to all nodes in the networks. The mobile ad hoc network uses routing protocol to deliver the packet and it is classified into three categories: proactive, reactive and hybrid routing protocol. AODV protocol is a kind of reactive routing protocol which uses RREQ (route request) and RREP (route reply) packet. The nodes of AODV routing protocol get compromised from various kind of attack in which one is black hole attack which broadcast itself that has optimal path for destination. In this paper security algorithm is used to determine and thwart the black hole node from the network.

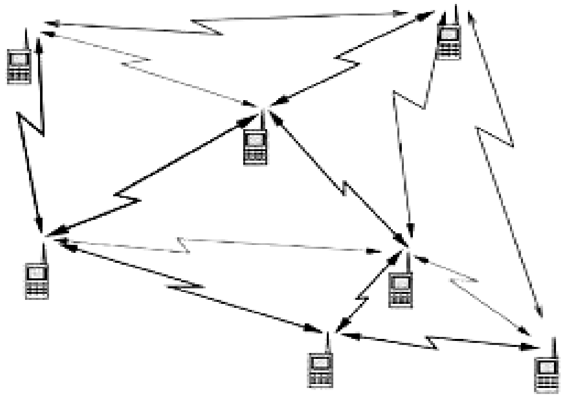

Fig. 1. Mobile ad hoc network architecture.

The experimental analysis of proposed system is perform on network simulator NS-2.34 and for measuring the performance PDR, throughput and end – to- end delay metrics is used. The remaining section of the paper is presented in this manner: Section 2 gives overview of the black hole attack in AODV and in next section presented the literature study of formerly work done for detection of black hole attack. Section describes the proposed methodology for black hole detection. The experimental result and its analysis is described in section V and section last not least concluded our paper.

II. BLACK HOLE ATTACK IN AODV PROTOCOL

Black hole attack [10] is hazardous active attacks on the Mobile Ad hoc Networks. A black hole attack is performed by a single node or amalgamation of nodes as shown in figure 1. This invader node is also called selfish node. In Black hole attack an invader node sends a counterfeit Route reply (RREP) message to the source node which commences the route discovery procedure order to find the route to the destination node. When the source node received multiple RREP, it chooses the greatest one as the most recent routing information and selects the route contained in that RREP packet [11]. In case the sequence numbers are equal it chooses the route with the smallest hop count. The attacker spoofed the uniqueness to be the destination node and directs RREP with destination sequence number higher than the real destination node to the source node. Formerly the attacker drops all data packets rather than forwarding them to the destination node.

As per shown in Figure 2 below, source node 1 broadcasts an RREQ message to ascertain a route for sending packets to destination node 3. An RREQ broadcast from node 1 is received by neighboring nodes 2, 4 and 5. Nevertheless, malevolent node 5 sends an RREP message instant onerously deprived of even having a route to destination node 3. The RREP message sent by the malicious attacker node is the first message reaches to the source node. As soon as the source node accept the message sent by the malevolent attacker node, updates its routing table for the new route for the intended destination node and formerly also discards any RREP message from other neighboring nodes even from an actual destination node. As soon as the Source node acquires the route, it starts sending the buffered data packets instantly from that route which is provided by the malevolent attacker node. Nonetheless, a Black hole node drops all data packets rather than forwarding them on.

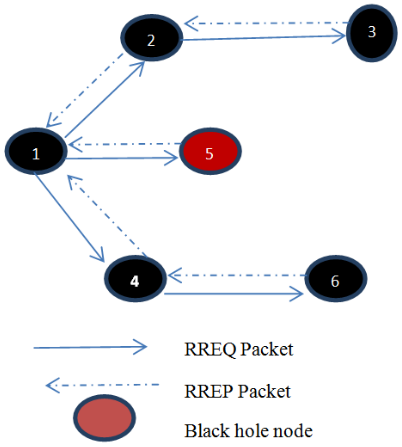

Fig. 2. Black hole attack in AODV.

III. RELATED WORK

Security is the major issues in mobile ad hoc network and lots of work has been done for detection and removal of black hole in network in which some of the methodologies is explained below:

Vanitha *et al.* [3] proposed a probabilistic misbehavior detection scheme is highly desirable to assure the secure DTN routing as well as the establishment of the trust, among DTN nodes. A zone (routing zone) of a node is used to collect the node information within the range. In this protocol, it cannot achieve the packet delivery ratio, performance and data loss rate. This paper is providing the explanation alongside black hole attack which is based on fuzzy rule. Fuzzy rule is used to ascertain the infected node as well as deliver the solution to diminish data loss over network. Fuzzy logic ranges between the value as {0, 1}. Geographic routing is one of the most suitable routing strategies in wireless mobile Ad hoc network mainly due to its scalability. Multi Input Multi Output technique used to send data frequently in routing protocol. Analysis and simulation results demonstrate the effectiveness and efficiency of the drop node analysis, high packet delivery ratio, throughput and delay. Kaur *et al.* [4] proposed a method to design a mechanism of blackhole detection based on artificial neural networks (ANNs). Using a simulated MANET environment, ANNs modeling for detecting the black hole attack is investigated and it is showed that model can detect nodes under blackhole attack effectively.

Sakuna *et al.* [5] used that source node will broadcast RREQ to other nodes till a destination node or node which have a route to destination replies RREP back to source. The receiving node will assign a credit to the next hop node or who sent RREP. When a node in the path sends one packet, one credit is deducted from the next hop node. As soon as a destination node receives data packet, it will send Credit Acknowledge (CACK) and it will back to a source node. A node within a way back will increase credit of the next hop by 2 to indicate a higher trust level of the next hop. On the other hand, credit will be decreased if a node cannot receive CACK. The node will be un-trusted and mark as a blacklist, when a credit reaches zero. Narang *et al.* [6] proposed fuzzy based approach which used these two factors to solve the problem. Definite conclusion based on ambiguous noisy or missing information. First we define the N number of nodes and set source and destination node and repeat step un till current node equal to destination node with using neighbor nodes and keep record of each neighbor node. Algorithm is on priority high priority node will take part in communication. Priority pronounce by subsequent step 1) packet loss is low and data rate is high set high priority 2) packet loss is medium and data rate is great set medium priority 3) Packet loss and data rate both low set low priority. Patro *et al.* [7] proposed a security measure to black hole attack on AODV based MANETs. It is one of the active DOS in which malevolent node imitates a destination node by sending a forged RREP to the source node. They studied the black hole attack by the existence of single malevolent node in the network and its solution proposed by different authors. Review of proposed solutions suggested that the performance of the routing protocol is affected in terms of additional overheads, end-to-end delay and packet delivery ratio. Howarth *et al* [8] proposed a survey of MANET intrusion detection and prevention approaches for network layer attacks. This enables a protection mechanism to learn from experience and use the existing knowledge of attacks to infer and detect new intrusive activities. Protection mechanism needs to robust enough to protect them and not introduce new vulnerabilities into the system. Singh *et al.* [9] proposed a method in which broadcast synchronization (BS) and relative distance (RD) method of clock synchronization is used to prevent the black hole nodes. In this internal and external clock node compare with the threshold clock if both the clock time is greater than the threshold then it is found that the node is malicious. This method can easily detect and prevent the block-hole node.

IV. PROPOSED WORK

From the discussion of the security attacks, we can say that MANET is vulnerable to the malicious activities. Using a strong authentication algorithm along with an encryption technique can overcome the security problems. Therefore, we have chosen DSA (Digital Signature Algorithm) for authentication purpose and Blowfish algorithm for encryption.

A. Digital Signature Algorithm (DSA)

Digital Signature Algorithm (DSA) [13] is based on logarithmic computations and therefore hard to break in. The requirements for DSA are classified into four categories.

Global public key component (p, q, g): p is a prime number ranging $2\ L\text{-}1 < p < 2\ L$ where L is the bit length of p ranging from $512 \leq L \leq 1024$ and integer multiple of 64. q is a prime divisor of (p-1) where $2\ 159 < q < 2\ 160$. g is a generator of the subgroup of the order q mod p such that $1 < g < p$.

Users' private key (x): x is a random or pseudorandom integer ranging $0 < x < q$.

Users' public key (y): $y = g\ x \bmod p$

Users' per message secret number (k): k is a random or pseudorandom integer ranging $0 < k < q$.

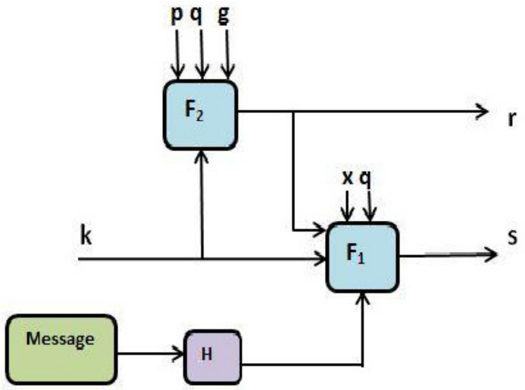

Fig. 3. Signing in DSA (sender).

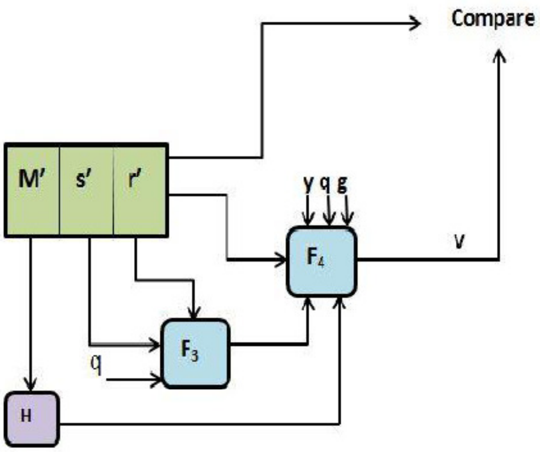

Fig. 4. Verification Process (receiver side).

DSA algorithm has two stages. In the first stage, message is signed by the sender. Fig. 3 represents the signature process and functions in DSA in sender side. This signature (r, s) along with the message (M) is transmitted to the receiver. The receiver receives a triplet of { M', r', s'} where M', r', s' are the received versions of M, r and s respectively. The second stage occurs at receiver side by verifying the signature of the message shown in Fig. 4. The different functions used in different stages are shown in Table 1.

Table 1: Functions used in DSA.

Signing	r = F2(k, p, q, g) = (g k mod p) mod q s= F1(H(M), x, r, q, k) = (k - 1(H(M) + xr)) mod q Signature= (r, s)
Verification	w = F3(s', q) = (s') -1 mod q v = F4(y, p, g, w, r', H(M')) = [(g [H(M')w] mod q y (r')w mod q) mod p] mod q Test v = r'

B. Blowfish Algorithm

Blowfish a symmetric key block cipher using 64 bits of data blocks and a variable size key maximum up to 448 bits. It comprises of Feistel Network having 16 times iterative operations of a simple encryption function. The prime characteristics of Blowfish algorithm is that it includes key dependent S-boxes and has a complex key schedule which makes the algorithm stronger.

Encryption. The data block of 64 bits are first divided into two halves of 32 bits each. Each line in the diagram of the Blowfish algorithm represents 32 bit data. It uses two sub key arrays 18-entry P-array and 256-entry S-boxes. The S-boxes convert the 8 bit input into 32 bits output. One entry of P-array is compulsory for each of 16 rounds as shown in the Fig. 5. The remaining two P-array entries are used after the final round to separately XOR the outputs of each of the halves of the data block of 32 bits. In the function F, four S-boxes and two types of bit operations: XOR and addition of modulo 2 32 are used. The function F first divides the input of 32 bits into four S-boxes of consisting 8 bits each. The outputs of first and second S-boxes are first added to modulo 2 32 and the output is XOR ed with the third S-box output. The result of XOR operation and the output of fourth S-box are finally added to modulo 2 32 and we get the final 32 bit output from the function F. The round function operation is shown in Fig. 6.

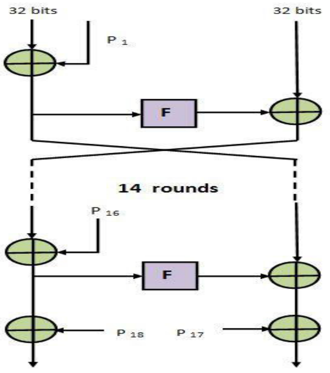

Fig. 5. Blowfish Algorithm.

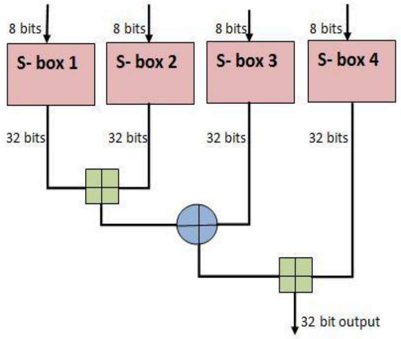

Fig. 6. Round function F in Blowfish.

The key schedule of Blowfish algorithm starts by initializing the P-array and S-boxes with values derived from the hexadecimal value of pi (Π). The secret key is then byte wise XOR-ed with all the P-entries in order. Many implementations may support 576 bit key size asthe P-array is 576 bits long (18 * 32 bits) and the bytes are XOR-ed with all these bits.

Decryption. Decryption is exactly the same as encryption technique except the P1, P2 .... P18 are used in reverse order.

C. Merging of Blowfish and DSA

In wireless network environment messages or data are transmitted in form of packets. The attacks in the MANET environment are due to basically fabrication or modification in data and unauthorized mobile node interception. So, it is needed to utilize the both authentication and encryption. The sender creates a data packet and encrypts with Blowfish Algorithm. The encrypted data is then digitally signature by the sender where a random number is generated per message and keep secret. So, any other third party cannot break through it as the secret number is unknown to the third party. To gain access to the message the third party must need the secret number. So, authentication and encryption both are utilized to make the transmission secure enough.

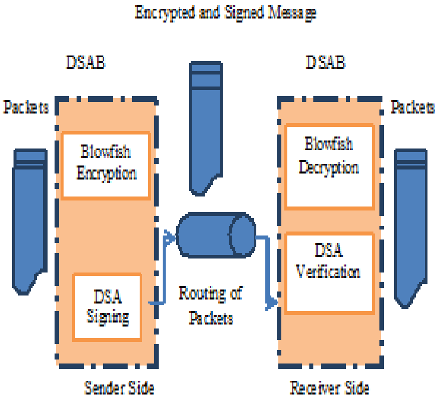

Fig. 7. Working of DSAB in Routing.

The Blowfish Algorithm:

-Manipulates data in large blocks
-It has a 64-bit block size.
-It has a scalable key, from 32 bits to at least 256 bits.
-It uses simple operations that are proficient on microprocessors. *e.g.,* exclusive-or, addition, table lookup, modular- multiplication. It does not use variable-length shifts or bit-wise permutations, or conditional jumps.
-Exercises pre computable sub-keys. On large-memory systems, these sub-keys can be pre-computed for fast reoperation. Not pre-computing the sub-keys will outcome in slower operation, but it should still be probable to encrypt data deprived of any pre-computations.
-It comprises of a variable number of iterations. For applications with a small key size, the trade-off among the complexity of a brute-force attack and a differential attack make an outsized number of iterations superfluous. Henceforth, it should be possible to diminish the number of iterations with no loss of security (outside that of the reduced key size).
-Utilizes sub-keys that are a one-way hash of the key. This allows the use of long passphrases for the key without compromising security.
-It has no linear structures that moderate the complexity of extensive search.
-It uses a design that is simple to comprehend. This accelerates analysis and upsurge the confidence in the algorithm. In practice, this means that the algorithm will be a Feistel iterated block cipher.

V. EXPERIMENTAL RESULT & ANALYSIS

Simulation is a fundamental tool in the development of MANET protocols, because the difficulty to deploy and debug them in real networks. The simulation eases the analyzing and the verification of the protocols, mainly in large-scale systems. It suggests bendable testing with dissimilar topologies, mobility patterns, and numerous physical and link-layer protocols. Nevertheless, a simulation cannot offer indication in real-world scenarios, owing to conventions and simplifications that it makes. Consequently, the results obtained from the simulations should be evaluated appropriately. The well-known simulators are used for MANET simulations: NS-2.34, GloMoSim and OPNET. We selected NS-2.34, because firstly it is very dynamic and also scalable simulator that is designed particularly to large wireless networks. It supports hundreds of nodes, using parallel and distributed environment.

A. Simulation Environment

The NS-2.34 Network Simulator [12] is an open-source object-oriented discrete-event simulator for network research. The simulator is written in C++, with an OTcl (Object Tool Command Language) interpreter used as the command interface. The C++ part constitutes the core of the simulator, where detailed protocol implementation and the simulation engine are located.
We modeled network traffic using Constant Bit Rate (CBR) sources. A CBR traffic source provides a constant stream of packets throughout the whole simulation, thus further stressing the routing task. In each experiment, half the nodes in the network are CBR sources, and each source transmits 64-byte packets at a rate of 4 per second. We experimented with higher sending rates, packet sizes and number of sources. We omit those results, as they show similar trends, with the predictably higher effect of network congestion.

Table 2: Simulation Setup.

Simulation used	NS-2.34
Topology area	1000 X 1000
No. of Mobile Nodes	50
Simulation Time	250
Speed	45 m/sec
Packets	CBR
Black hole	1, 2, 3
Protocol	AODV, Black hole AODV, IDSAODV

A. Result Analysis

The results of simulation are given in the Figures. The performance of the network is analyzed in terms of four metrics such as packet delivery ratio, throughput, routing load and end to end delay.
The simulation performance for packet delivery ratio of black hole node and our work is done and it is observed that the PDR of our proposed work is about 78% after varying the simulation time. The simulation result of PDR is shown in table 3 and the comparison is shown through Fig. 8.

Table 3: Simulation result of PDR.

PDR Performance				
Time	B0	B1	B2	Proposed
1	0	0	0	27
20	99.712	56.559	21.351	81.512
40	98.679	55.237	19.289	84.655
60	99.375	53.629	18.313	85.213
80	94.107	52.906	17.789	84.795
100	90.095	51.846	17.427	84.145
120	86.999	51.418	17.244	83.778
140	85.59	51.618	17.107	83.312
160	82.817	51.733	17.616	83.213
180	80.964	51.768	17.993	83.203

Average PDR Performance			
B0	B1	B2	Proposed
81.8338	47.6714	16.4129	78.0826

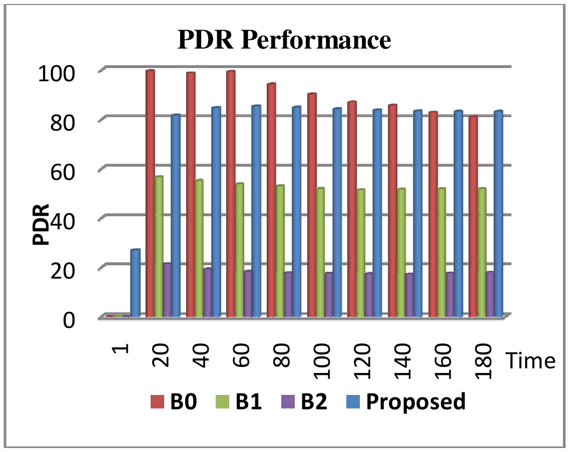

Fig. 8. Analysis for PDR of proposed work.

Table 4: Simulation result of Throughput.

Throughput Performance				
Time	B0	B1	B2	Proposed
1	2	8	2	4
20	70.008	61.476	4.925	94.45
40	74.872	51.3076	4.688	94.45
60	81.379	42.397	4.604	94.45
80	83.135	39.269	4.59	94.45
100	84.996	39.864	4.562	94.45
120	87.773	39.236	4.559	94.45
140	91.431	38.65	4.572	99.535
160	94.456	36.81	4.556	93.038
180	94.033	34.049	4.567	88.003

Average Throughput Performance			
B0	B1	B2	Proposed
76.4083	39.10586	4.3623	85.1276

The analysis & performance for throughput of black hole node and proposed work is perform and it is observed that the throughput of our proposed work is about 85% by varying the simulation time. The simulation result of throughput is shown in table 4 and the comparison is shown through Fig. 9.

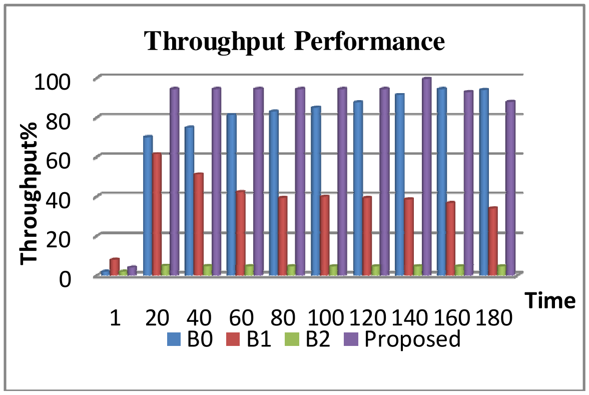

Fig. 9. Analysis for Throughput of proposed work.

Table 5: Simulation result of Routing Load.

Routing Load Performance				
Time	B0	B1	B2	Proposed
1	0	0	0	0
20	3.2	21.4	3.9	2.2
40	5.9	34.2	4.8	3.2
60	10	45.7	9.9	3.9
80	13	45.8	14.6	5
100	15.2	46	16.7	5.6
120	16.4	46.1	19	6.3
140	16.6	46.2	21.6	6.5
160	17	46.6	24	7.1
180	17.8	47	25.9	7.2

Average Routing Load Performance			
B0	B1	B2	Proposed
11.51	37.9	14.04	4.7

The analysis & performance for routing load of black hole node and proposed work is perform and it is observed that the network routing load of our proposed work is about 4.7% by varying the simulation time which means that our method reduces the network load than other one. The simulation result of routing load is shown in table 5. and the comparison is shown through Fig. 10.

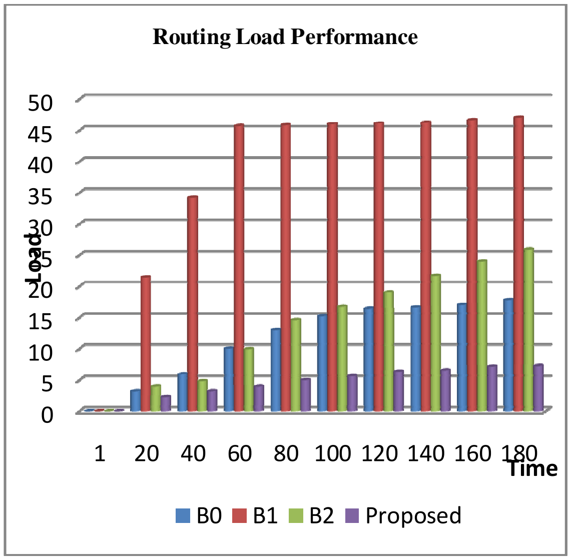

Fig. 10. Analysis for Routing Load of proposed work.

The analysis & performance for end to end delay of black hole node and proposed work is perform and it is observed that the delay of our proposed work is about 2.7% by varying the simulation time which means that our method reduces the end to end delay than other one. The simulation result of routing load is shown in table 5.5 and the comparison is shown through Fig. 11.

Table 6: Simulation result of Routing Load.

End to End Delay Performance				
Time	B0	B1	B2	Proposed
1	1.38	178.6	83.32	1.38
20	2.34	164.72	272.81	3.6
40	2.16	164.72	248.02	3
60	2.6	99.33	252.93	2.76
80	2.75	164.72	269.84	2.85
100	2.65	124.36	286.16	2.3
120	2.55	117.3	263.1	3.04
140	2.85	124.36	299.51	2.37
160	3.04	99.33	286.83	2.52
180	2.87	178.6	272.91	3

Average End to End Delay Performance			
B0	B1	B2	Proposed
2.519	141.604	253.543	2.682

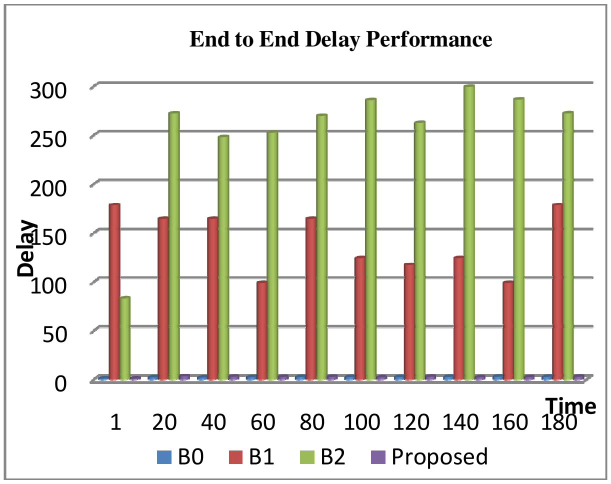

Fig. 11. Analysis for End to End delay of proposed work.

CONCLUSION

Wireless ad hoc network is infrastructure less network and because of this number of attacker gets compromised from these nodes which can discard or drop the packets. In this, we suggested a security algorithm using blowfish and digital signature to thwart the black hole node. The experimental result of our proposed methods outperforms than the existing one but this approach is more complex in design so in future work develops such approach which is less complex and produces less overhead.

REFERENCE

[1]. X. Wu and D. K. Y. Yau, (2007). "Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach", *In Proc. 3rd International Conference on Security and Privacy in Communications Networks, Nice,* France, September 2007.

[2]. Lalita Prajapati, Anurag Singh Tomar (2015). "Detection of Black Hole Attack With Improved AODV Protocol in MANET", *International Journal of Innovative Research in Science, Engineering and Technology,* Vol. **4**, Issue 5, May 2015.

[3]. S. Karthika, N. Vanitha, (2015). "Secure Routing Protocol in Delay Tolerant Networks using Fuzzy Logic Algorithm", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,* Vol. **4**, Issue 5, May 2015.

[4]. Ramanpreet Kaur and Anantdeep Kaur (2014). "Blackhole Detection In Manets Using Artificial Neural Networks", *International Journal For Technological Research In Engineering,* Volume **1**, Issue 9, May-2014.

[5]. Watchara Saetang and Sakuna Charoenpanyasak, (2012). “CAODV Free Blackhole Attack in Ad Hoc Networks”, 2012 *International Conference on Computer Networks and Communication Systems (CNCS 2012).*

[6]. Sonal, Kiran Narang (2013). “Black Hole Attack Detection using Fuzzy Logic” 2013. *International Journal of Science and Research (IJSR),* ISSN: 2319-7064.

[7]. Subash Chandra Mandhata, Dr. Surya Narayan Patro, (2011). “A Counter Measure to Black hole Attack on AODV Based Mobile Ad hoc Networks”, *International Journal of Computer & Communication Technology (IJCCT),* Vol. **2**, Issue 6, 2011.

[8]. Adnan Nadeem and Michael P. Howarth, (2013). “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, *IEEE Communication Surveys & Tutorials, accepted for publication, 2013.*

[9]. Harsh Pratap Singh, Rashmi Singh, (2014). “A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol”, *International Conference on Electronics and Communication Systems (ICECS)* 2014, Page(s):1-8 Print, ISBN: 978-1-4799-2321-2.

[10]. Neelam Khemariya, Ajay Khuntetha, (2013). “An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs”, *International Journal of Computer Applications,* Volume **66**, No.18.

[11]. K. Lakshmi, S. Manju Priya, A. Jeevarathinam K. Rama, K. Thilagam, “Modified AODV Protocol against Blackhole Attacks in MANET”, *International Journal of Engineering and Technology.*

[12]. http://www.isi.edu/nsam/ns.

[13]. W. Stallings, (2005). "Cryptography and Network Security 4th Ed," Prentice Hall, 2005, PP. 58-309.