International Journal of Electrical and Computer Engineering (IJECE)
Vol.8, No.6, December 2018, pp. 4412~4422
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp4412-4422 

# Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET

**Jeenat Sultana[1], Tasnuva Ahmed[2]**
[1]Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Bangladesh
[2]Department of Computer Science and Engineering, Southern University Bangladesh, Bangladesh

**Article Info**

***Article history:***

Received Oct 12, 2017
Revised Jul 4, 2018
Accepted Jul 18, 2018

***Keyword:***

AOMDV
Cryptography
NS-2.5
Security

**ABSTRACT**

Mobile nodes roaming around in the hostile environment of mobile adhoc network (MANET) play the role of router as well as terminal. While acting as a router, a node needs to choose a reliable routing protocol. Besides, an encryption algorithm is needed to secure data to be conveyed through the unfriendly atmosphere while acting as a terminal. We have implemented Elliptic Curve Cryptography (ECC) along with Adhoc On Demand Multipath Distance Vector (AOMDV) routing protocol to secure data transmission against blackhole attack in a MANET. ECC, a public key cryptography that works on discrete logarithm problem with a much smaller key size, has been used to encrypt data packets at source node before transmission. We have used AOMDV, a reliable routing protocol compared to its parent protocol, Adhoc On Demand Distance Vector (AODV), with a multipath extension, for routing. The encrypted packets transferring between nodes via AOMDV, has been proved secured against blackhole attack. The performance of the secured protocol has been analyzed in terms of different performance metrics and in terms of varying number of blackhole attacker nodes.



***Corresponding Author:***

Jeenat Sultana,
Department of Computer Science and Engineering,
Southern University Bangladesh,
22 Shaheed Mirza Lane (E), Mehedibag Road, Chittagong 4000, Bangladesh.
Email: swarna0404056@yahoo.com

## 1. INTRODUCTION

A Mobile Ad-hoc network (MANET) consists of a number of nodes communicating in an infrastructureless manner using the radio frequency channel. Besides playing the role of a terminal, every node needs to act as router. The protocols used for data transmission in MANET assume a trusted environment and thus security issues are not in built. The environment can be considered adversary as data transmitted by a source node can be collected by a compromised node within its direct transmission range. Security might be achieved by avoiding the attacker nodes through intrusion detection techniques. The other way is to secure the data to be transmitted over a hostile environment so that the data is kept protected even after attack. Following the second technique, we have used Elliptic Curve Cryptography (ECC) along with Adhoc on Demand Multipath Distance Vector (AOMDV) protocol and have shown the impact on blackhole attack.

Mobile nodes travelling in mobile adhoc networks are vulnerable to attacks. Thus, security becomes a very sensitive issue in MANET. To ensure secure transmission, various encryption algorithms have already been used with various protocols. Still the fragile nature of the protocols does not let them keep data transmission secure for a long period of time. In this work, we have shown the impact of ECC based AOMDV on blackhole attack and analyzed its performance using various performance metrics in respect of time and against varying number of blackhole attacker nodes. In the previous work [1], we only dealt with

the performance against time. Sonal Shrivastava et al [2] proposed a scheme of Intrusion Detection System (IDS) that uses a hop count mechanism to detect the attacker. The proposed IDS scheme keeps record of the routing information, the intermediate node that receives the data, the next hop of that node. It gathers the attacker information, forwards to the network and defends further participation. Vandana Arora et al [3] presented a trusted and authenticate environment that is created by RSA based signature and implemented with AODV protocol. They have used RSA encryption algorithm that uses a larger sized key and the routing protocol, AODV provides no multipath facility. Priyanka Bansal et al [4] study the effect of blackhole attack and neighbor attack on AOMDV protocol. Any solution to the attacks has not been proposed. M Janardhana Raju et al [5] proposed a system based on Elliptic curve ElGamal Encryption technique and used it with AODV. In our proposed system, we emphasized on the encryption algorithm that is more secure and the protocol, AOMDV with less overhead.

The rest of the paper is organized as follows; Section 2 discusses the properties of AOMDV protocol, blackhole attack, the detail of Elliptic Curve Cryptography (ECC), the reasons behind choosing AOMDV as routing protocol and ECC as encryption technique, the later of this section is about the methodology and contribution, section 3 shows the simulation scenario and results and performance analysis of AOMDV before and after security implemented. In section 4, we conclude our work with future scope.

## 2. RESEARCH METHOD

### 2.1. Properties of AOMDV

The key of the AOMDV protocol lies in ensuring that multiple paths discovered are loop-free and disjoint. The route discovery is maintained by a flood-based mechanism. AOMDV route update rules are implemented to every node in order to maintain loop-freedom and disjointness. AOMDV uses the routing information already available in the basic AODV protocol [6], thereby reducing the overhead caused while discovering multiple paths [7]. The properties that are maintained by AOMDV protocol are as follows:

a. Loop Freedom

Loop freedom in AOMDV is maintained by the parameter 'Advertised_hopcount'. The advertised hopcount represents the maximum hopcount of the multiple paths for the destination available at the source node. The advertised hopcount remains constant for the same sequence number. The protocol only accepts alternate routes with lower hopcounts, thus guarantees loop freedom.

b. Disjoint Path

One of the following two types of disjoint paths is maintained by AOMDV protocol:

1. Node-disjoint path: The path that does not have any node in common.
2. Link-disjoint path: Link-disjoint paths do not have any common links. Though, link-disjoint paths may have nodes in common. Link disjointness is maintained by AOMDV as node-disjointness is much stricter than link-disjointness and presents lesser number of disjoint routes. Thus, is less effective.

c. Multiple Path Maintenance

AOMDV processes every RREQ packet to maintain multiple paths. While its parent node, AODV processes the first RREQ sent from a source node to create a communicating path between two nodes and discard the other ones.

d. Fresh route maintenance

AOMDV chooses routing path by considering the maximum sequence number and thus maintains fresh route. In case of same sequence number, it considers minimum hop count. The types of sequence number maintained by AOMDV are:

1. Source Sequence Number: Every node maintains a monotonically increasing sequence number.
2. Destination Sequence Number: Every node maintains the highest known sequence number for each destination in the routing table.

### 2.2. Blackhole Attack

Blackhole Attack is a kind of attack where the attacker node sends a false RREP as an answer to the RREQ and shows itself as a routing node with the freshest route by generating a larger sequence number. In this attack [8] [9], the adversary node attracts packets but does not transmit any packet to the destination, rather drops them all. Due to this attack the packets sends by the nodes do not reach their proposed destination. AOMDV generally chooses an alternate path when a path is blocked by an attacker node. The problem mainly occurs when every other path is blocked by a number of attacker nodes and the attacker node acting as a router camouflages itself as a valid one. The Figure 1 shows a MANET where the packet transmitted by the source, S destined for D is achieved by M, a blackhole attacker node playing the role of a router with greater sequence number. A, B and C are the intermediate nodes.

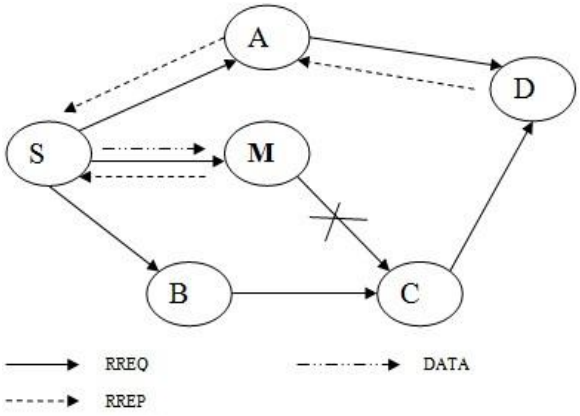


Figure 1. Blackhole attackRREQ: Route request, RREP: Route reply, seq_no: sequence number

### 2.3. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is used to describe a group of cryptographic tools and protocols where the security is based on the discrete logarithm problem. ECC is based on sets of numbers and equations that are associated with elliptic curves [10]. ECC works in the following phases:

a. Key Generation
1. Global Public Elements
   a) $E_p(a,b)$ elliptic curve with parameters a, b & p in the equation:$Y^2 \bmod p=(X^3+aX+b) \bmod p$
   b) G is the base point on elliptic curve
2. User A Key Generation
   a) Select private key $n_A$ ; $n_A<n$
   b) Calculate public key, $P=n_A \times G$
3. User B Key Generation
   a) Select private key, $n_B$ ; $n_B<n$
   b) Calculate public key, $M=n_B \times G$
4. Generation of Secret Key by user A, $P_1=k=n_A \times M$
5. Generation of Secret Key by user B,$P_2=k=n_B \times P$
   The two calculations produce the same result because $n_A \times M=n_A \times (n_B \times G)=n_B \times (n_A \times G)=n_B \times P$.

b. ECC Encryption
1. Consider a message 'Pm' sent from A to B.
2. User 'A' chooses a random positive integer 'k', a private key '$n_A$' and generates the public key,
3. $P_A=n_A \times G$.
4. Chooses G, the base point selected on the Elliptic Curve $E_p(a, b)$.
5. Produces the ciphertext, consisting of pair of points, $Cm=\{kG, Pm+kP_B\}=(C_1, C_2)$ where,
6. $P_B=n_B \times G$.
7. The public key of B with private key '$n_B$'.

c. ECC Decryption
1. To decrypt the ciphertext, Cm, B multiplies the first point in the pair, $C_1$ by B's secret key.
2. Subtracts the result from the second point, $C_2$, $Pm + kP_B - n_B (kG)=Pm + k (n_B G) – n_B (kG)=Pm$.

### 2.4. Why AOMDV?

AOMDV, Adhoc on Demand Multipath Distance Vector Protocol [7], is the multipath extension of the renowned AODV protocol. Being the multipath extended version, it provides more alternate paths and thus is more reliable. It reduces the overhead caused by link failure and route discovery. In AOMDV, route discovery is only needed when every alternate link is broken.

### 2.5. Why ECC?

Elliptic Curve Cryptography is a reliable and efficient public key cryptographic technique that provides equivalent security as other public key cryptographic techniques but with smaller key size [10], [11]. Moreover, It is based on the discrete logarithm problem [12] which states that if K=nxG, then it is easy to derive K with given n and G, but tough to reveal n with given K and G. Thus with ECC, it will be tough for the blackhole attacker node to retrieve the private key from given secret key and public key.

### 2.6. Methodology

The AOMDV protocol first discovers the multipath route to the destination through route discovery process and sends the packets to it. The flowchart of the discovery is shown in Figure 2. At the very beginning of data transmission, the source node broadcasts RREQ and the next hop that has route to the destination sends back RREP. On the contrary to AODV, AOMDV processes every RREQ. While AODV processes only the first RREQ and discards the rest. By processing every RREQ, AOMDV ensures multipath connectivity. The destination node chooses one of the multipaths by comparing the sequence number. The freshest route is guaranteed by considering the largest sequence number. In case of equal sequence number, path with less hop count is considered to ensure the shortest path. The destination forwards the RREP to the source node and the path is defined for data transmission.

After transmitting number of packets, AOMDV avoids the malicious node as it is designed so and restrains the source node from transmitting packets to the attacker node. In the meanwhile, some of the packets have already been retrieved by the attacker node. Our goal is to secure those retrieved packets from revealing. Thus to secure the data packets, the packets are encrypted by ECC. This is done by creating a secure agent that generates the encrypted packet. The packet is then reached the destination through one of the selected multipaths.

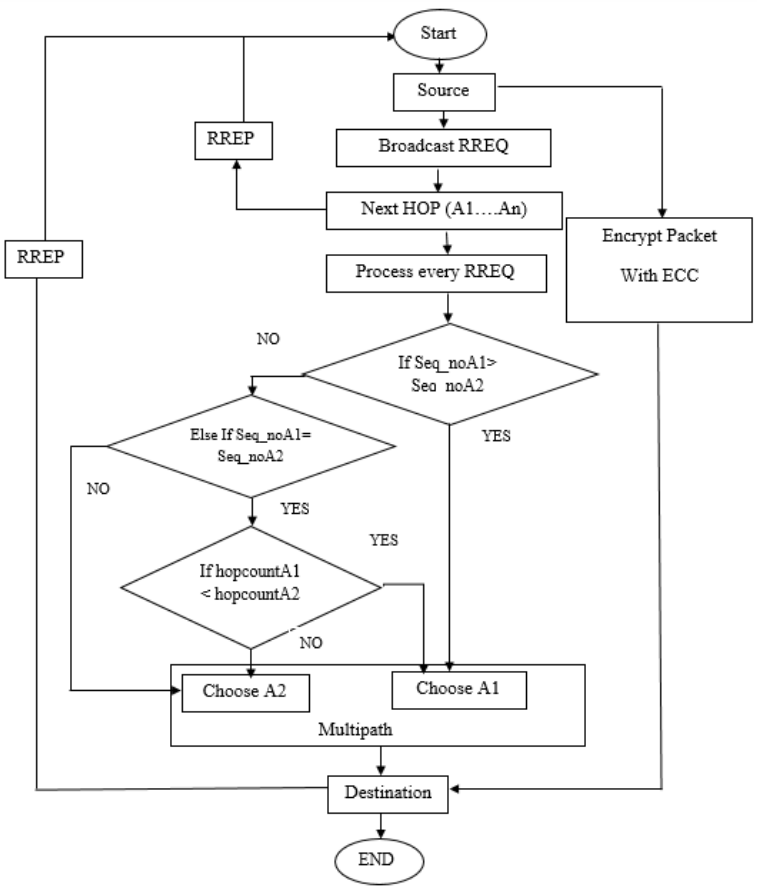


Figure 2. Flow chart of route discovery with AOMDV protocol. RREQ: Route request, RREP: Route reply, seq_no: sequence number

Every time a node works as a source, it generates a private/public key pair. Firstly, it chooses a random private key, generates a secret key from its own private key and receiver's public key. Then it encrypts the packet with the newly generated secret key and announces the public key. The encrypted packet is sent via AOMDV protocol. After receiving the encrypted packet, the destination node generates the same secret key with the help of its own private key and the sender's new public key. Then using its shared secret key and private/public key pair, the receiver decrypts the packet to get the original data as shown in Figure 3. It will be tough for the malicious node to retrieve the private key from given secret key and the public key.

Thus, if an attacker manages to reveal the secret key, it would be a challenge to retrieve the private key without which decrypting the packet is not possible.

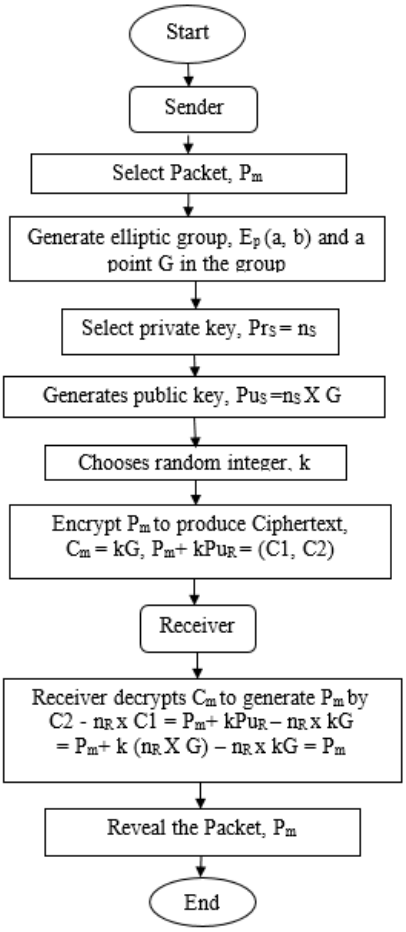


Figure 3. Packet encryption by ECC

## 3. RESULTS AND ANALYSIS

We have used NS-2.35 for the simulation of the proposed system, a discrete-event simulation instrument that has been proved functional in studying the vibrant nature of MANET. The performance is measured in three cases: without malicious node, with three blackhole attacker nodes and with ECC implementation.

The metrics that are used for analyzing the performance [5] of the protocol are described below:

a. Average Throughput

Average number of packets passing through the network per unit of time. It is measured in kbps.

$$\text{Average Throughput} = \frac{\text{Number of packets sent successfuly}}{\text{Time(in seconds)}}$$

b. Packet Delivery Ratio

It is the ratio of total number of packets successfully received at the destination nodes to the number of packets forwarded by the source nodes throughout the simulation.

$$\text{Packet Delivery Ratio} = \frac{\text{Number of Received Packets}}{\text{Number of Sent Packets}}$$

c. Average End-to-End Delay

This is the average delay between the sending of packets by the source and those received by the receiver.

$$\text{Average End-to-End Delay} = \sum_{i=0}^{n} \frac{(\text{Time of packet Recived - Time of Packet Sent})}{\text{Total Number of Packets Received}}$$

d. Normalized Routing Load

The number of routing packets transmitted per data packet delivered at the destination.

### 3.1. Simulation Scenario

In NS-2.35, we have considered an area of 1186 x 584 meters and the wireless topology we have used contains 25 nodes including 3 blackhole attacker nodes. The maximum speed of the mobile nodes is 0.1Mbps. The total time used for simulation is 100 seconds. The simulation scenario is shown in Table 1.

Table 1. Simulation Environment

| Simulation Parameter | Value |
|---|---|
| Simulator | NS-2.35 |
| Area | 1186 x 584 |
| Routing protocol | AOMDV |
| Attack | Blackhole attack |
| Packet size | 1000,1500 |
| Number of nodes | 25 |
| Number of attacker nodes | 3 |
| Traffic type | CBR,UDP |
| Node Placement | Random |
| Simulation time | 100 sec |

The output NAM file is shown in Figure 4 which is generated as a result of simulation. NAM stands for Network Animator that shows the graphical representation of packet transfer among the nodes in a MANET.

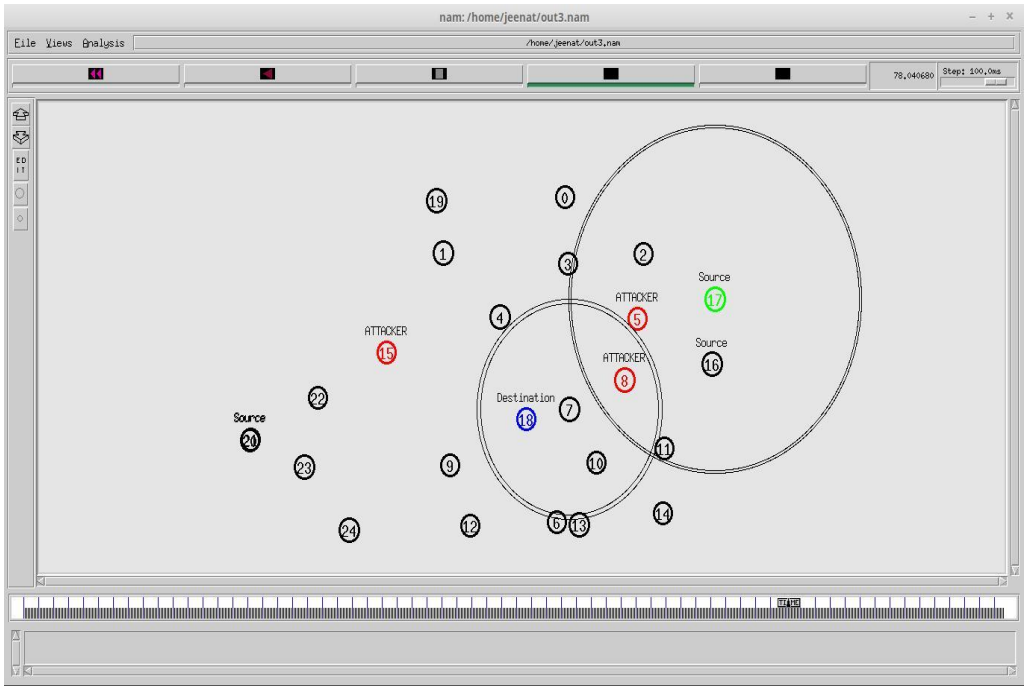


Figure 4. Output NAM file

In Figure 4, the blue node represents the destination, the sources are denoted by green and the red ones are the blackhole attacker nodes. Four source nodes are transmitting packets in time intervals of 20 seconds. From the generated trace files, different performance metrics are measured such as average throughput, end-to-end delay, packet delivery ratio and normalized routing load as shown in Table 2.

Table 2. Performance Analysis of AOMDV, with Attack and with Security

| Parameters | AOMDV without Malicious nodes | AOMDV with Blackhole Attack | AOMDV with ECC (against Blackhole Attack) |
|---|---|---|---|
| Total CBR packets sent | 1241 | 1241 | 1492 |
| CBR packets received | 1240 | 48 | 238 |
| Packet delivery ratio | 0.9992 | 0.0387 | 0.1595 |
| End-to-end delay (ms) | 85690.5 | 85656.3 | 85661 |
| Normalized Routing Load | 0.110 | 2.792 | 0.542 |
| Average Throughput (kbps) | 354.969 | 220.408 | 293.089 |

The data from Table 2 has been used to plot the performance metrics. The performance metrics are measured in every 10 seconds and is analyzed against time and number of malicious nodes consecutively.

### 3.2. Performance Analysis against Time

The curve in Figure 5 shows that the throughput without any malicious activity rises to about 355 kbps, the throughput dropped to about 220 kbps on the presence of malicious nodes. But with ECC implementation in the elementary AOMDV protocol, the values are increased to 290 kbps.


Figure 5. Time vs. throughput curve. nomal_th: Throughput with no malicious node, mal_th: Throughput with malicious node, sec_th: Throughput with security

As shown in Figure 6, the packet delivery ratio kept reducing on the presence of blackhole attacker nodes in the MANET and drops to about 0.04 with three attackers. But when the proposed method is implemented then even with the attacker nodes being present in the network, the packet delivery ratio improved considerably to above 0.15.

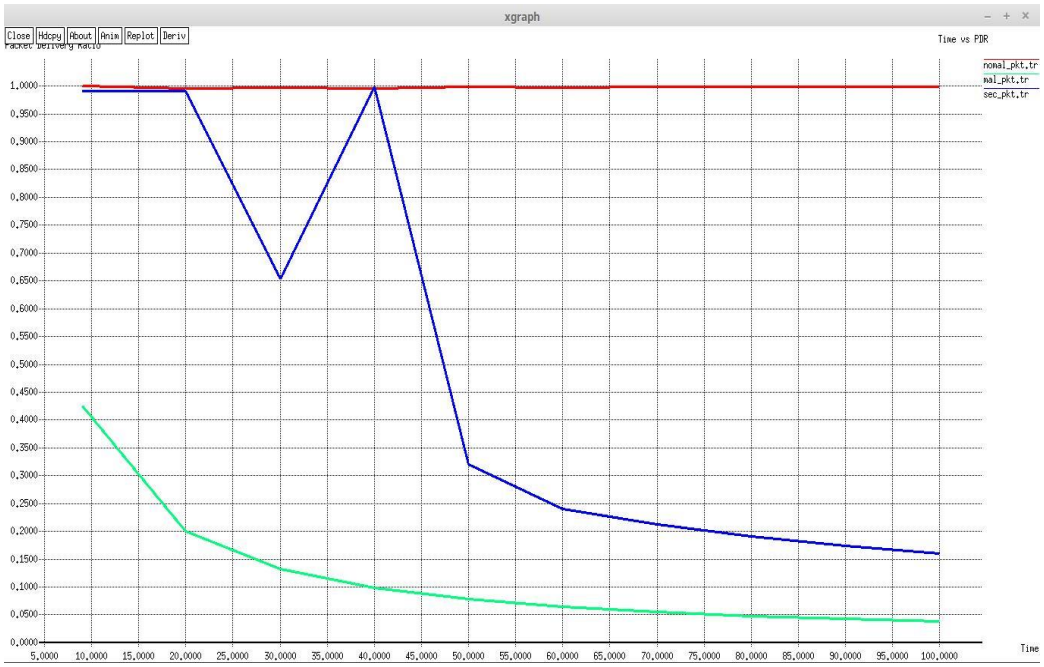


Figure 6. Time vs. packet delivery ratio curve. nomal_pkt: PDR with no malicious node, mal_pkt: PDR with malicious node, sec_pkt: PDR with security

The end-to-end delay is almost same in all the three cases as seen in Figure 7. Initially the delay is a bit higher with ECC implementation. On an average, the proposed method does not affect the end-to-end delay.

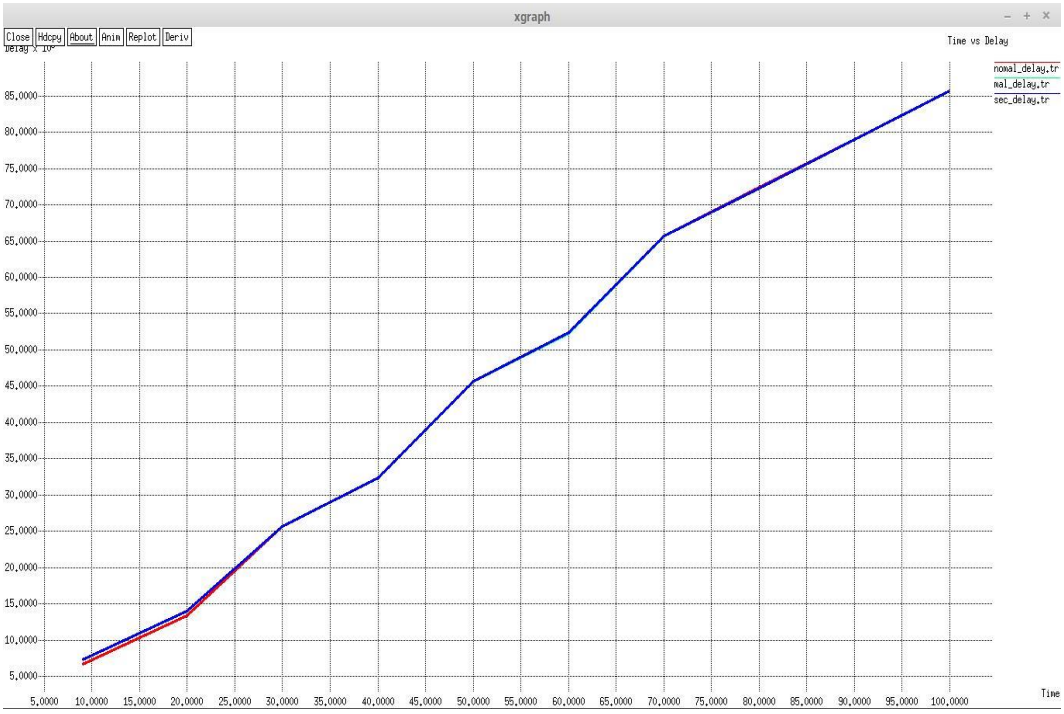


Figure 7. Time vs. delay curve. nomal_delay: End-to-end delay with no malicious node, mal_delay: End-to-end delay with malicious node, sec_delay: End-to-end delay with security

The graph in Figure 8 illustrated the normalized routing load for the three mentioned cases. The Normalized Routing Load is about 0.1 without attack; it raises high above 2.0 in the presence of attack and reduces to 0.5 with ECC implementation.

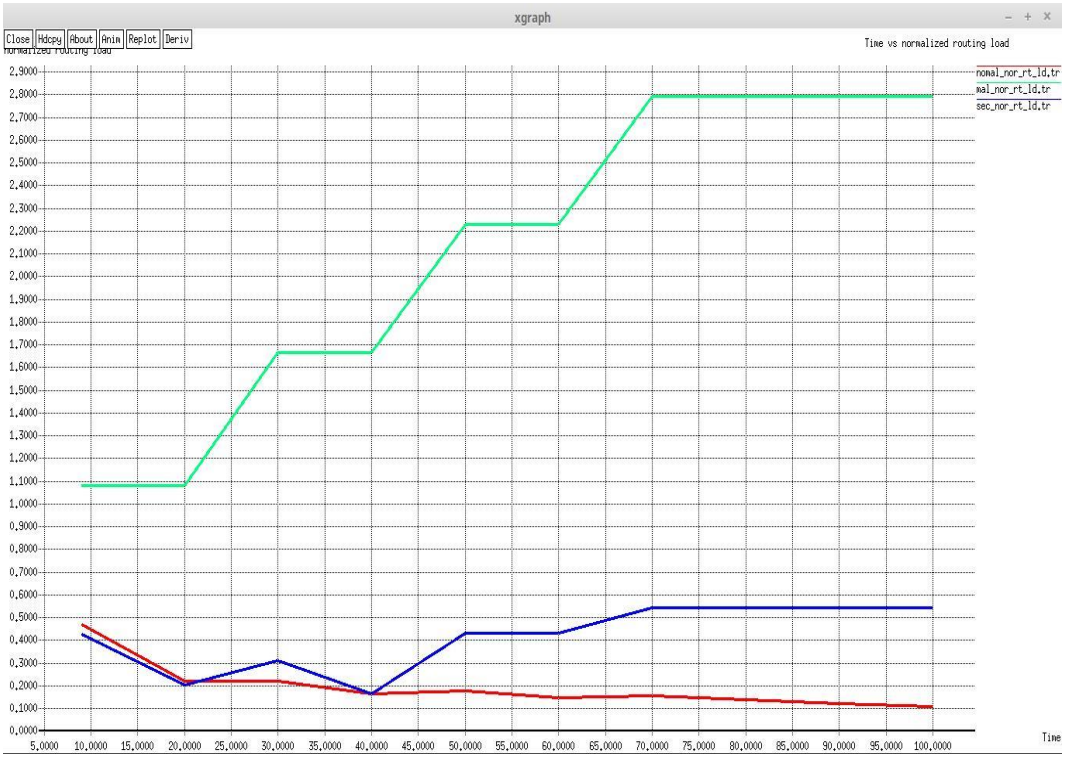


Figure 8. Time vs. normalized routing load curve. nomal_nor_rt_ld: Normalized routing load with no malicious node, mal_nor_rt_ld: Normalized routing load with malicious node, sec_nor_rt_ld: Normalized routing load with security

### 3.3. Performance Analysis against Number of Malicious Nodes

As in Figure 9, we observe that with varying number of malicious nodes, the average throughput doesn't decrease rapidly, instead with the newly developed protocol, the throughput changes very slightly.

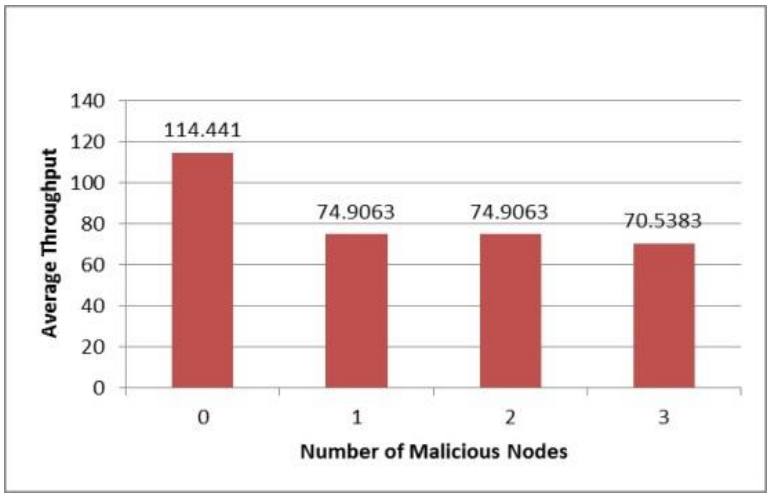


Figure 9. Number of malicious nodes vs. Average Throughput with secured AOMDV

The Packet Delivery ratio is definitely highest with no malicious node in the environment. It decreases slowly with increasing number of malicious nodes as in Figure 10. The average end-to-end delay shown in Figure 11 increases gradually with incremented malicious nodes as time is taken by the encryption process with ECC.

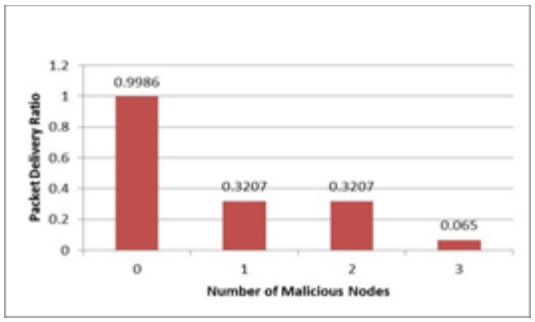


Figure 10. Number of malicious nodes vs. Packet Delivery Ratio with secured AOMDV

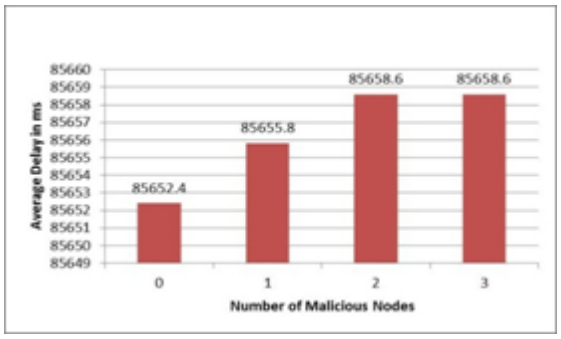


Figure 11. Number of malicious nodes vs. Average Delay with secured AOMDV

As shown in Figure 12, the normalized routing load grows with the number of blackhole attacker nodes present in the situation, though the normalized routing load may vary depending on the number of packet transmission.

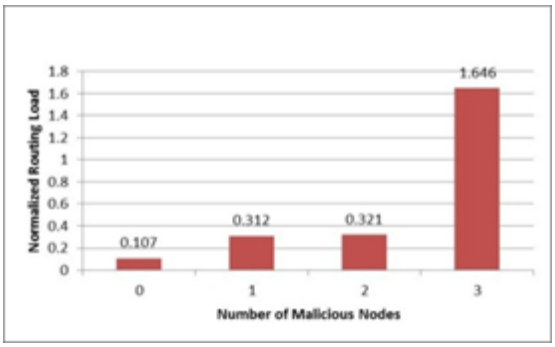


Figure 12. Number of malicious nodes vs. Normalized Routing Load with secured AOMDV

## 4. CONCLUSION

A MANET is subject to a variety of attacks. This paper proposes a way to secure data transmission in MANET so that data may remain confident when a negotiated node gets its proprietary. We have chosen blackhole attack, a very common one, to analyze the impact of secured AOMDV, though security is needed

to be imposed on every other attack. An intrusion detection system (IDS) along with proposed system may strengthen the security. We chose ECC considering its efficiency over other encryption protocols.

## REFERENCES


[1] Jeenat Sultana, Tasnuva Ahmed, "Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography", in *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, IEEE, 2017.

[2] Shrivastava Sonal, Chetan Agrawal, and Anurag Jain, "An IDS scheme against black hole attack to secure AOMDV routing in MANET", *International Journal on AdHoc Networking Systems*, vol. 5, 2015.

[3] Arora Vandana, Ahuja Sunil, "Trusted key management with RSA based security policy for MANETs", *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 2.

[4] Bansal Priyanka, Gupta Anuj K,"Impact of black hole and neighbor attack on AOMDV routing protocol", *International Journal of Innovations in Engineering and Technology*, vol. 3, pp. 90-99, 2014.

[5] Raju M Janardhana, Subbaiah P., Ramesh V., "A novel elliptic curve cryptography based AODV for mobile ad-hoc networks for enhanced security", *Journal of Theoretical and Applied Information Technology*, vol. 58, pp. 549-557, 2013.

[6] A. Peda Gopi, E. Suresh Babu, C. Naga Raju and S. Ashok Kumar, "Designing an adversarial model against reactive and proactive routing protocols in MANETS: A comparative performance study", *International Journal of Electrical and Computer Engineering*, vol. 5, pp. 1111-1118, 2015.

[7] Marina, Mahesh K., and Samir R. Das, "Ad hoc on-demand multipath distance vector routing", *Wireless communications and mobile computing*, vol. 6, pp. 969-988, 2006.

[8] Bhardwaj Neetika and Rajdeep Singh, "Detection and avoidance of blackhole attack in AOMDV protocol in MANETs", *International Journal of Application or Innovation in Engineering & Management*, vol. 3, pp. 376-383, 2014.

[9] Pradeep Kumar K, B.R. Prasad Babu, "Investigating open issues in swarm intelligence for mitigating security threats in MANET", *International Journal of Electrical and Computer Engineering*, vol. 5, pp. 1194-1201, 2015.

[10] Lauter, Kristin, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless communications*, vol. 11, pp. 62-67, 2004.

[11] K Renuka, G. Murali, "Providing security for multipath routing protocol in wireless sensor networks", *International Journal of Research in Engineering and Technology*, vol. 4, pp. 47-50, 2015.

[12] Samta Gajbhiye, Monisha Sharma, Samir Dashputre, "A survey report on elliptic curve cryptography", *International Journal of Electrical and Computer Engineering*, vol. 1, pp. 195-201, 2011.


## BIOGRAPHIES OF AUTHORS

Jeenat Sultana achieved B.Sc. Engg. Degree in Computer Science and Engineering from Chittagong University of Engineering and Technology in 2009 and MSIT degree in Computer Science and Information Technology from Southern University Bangladesh in 2016. She is now serving as a lecturer, Department of Computer Science and Engineering in Southern University Bangladesh. Her area of interests includes Mobile Adhoc Network, Network Security and Cryptography.

Tasnuva Ahmed achieved her B.Sc.Engg. degree in Computer Science and Engineering in 2006 from International Islamic University Chittagong and MSIT degree from Dhaka University in 2010. Currently, she is working as Assistant Professor, Department of Computer Science and Engineering, Southern Universuty Bangladesh. Her research interests include Network Security, Image Processing, Computer Vision and Machine Learning. She has published 3 papers in various international journals and confererences.