Detection and Prevention of Blackhole node

Fahmina Taranum, Ayesha Sarvat, Nooria Ali and Shamekh Siddiqui
Department of Computer Science and Engineering,
Muffakham Jah College of Engineering and Technology,
Hyderabad, India.

ftaranum@mjcollege.ac.in, ayeshasarvat1@gmail.com, nooriaali2020@gmail.com, shamekh.siddiqui@gmail.com

Abstract— **Mobile Adhoc networks (MANETs) comprises of mobile devices or nodes that are connected wirelessly and have no infrastructure. Detecting malicious activities in MANETs is a challenging task as they are vulnerable to attacks where the performance of the entire network degrades. Hence it is necessary to provide security to the network so that the nodes are prone to attack. Selecting a good routing protocol in MANET is also important as frequent change of topology causes the route reply to not arrive at the source node. In this paper, R-AODV (Reverse Adhoc On-Demand Distance Vector) protocol along with ECC (Elliptic Key Cryptography) algorithm is designed and implemented to detect and to prevent the malicious node and to secure data transmission against blackhole attack. The main objective is to keep the data packets secure. ECC provides a smaller key size compared to other public-key encryption and eliminates the requirement of pre-distributed keys also makes the path more secure against blackhole attacks in a MANET. The performance of this proposed system is simulated by using the NS-2.35 network simulator. Simulation results show that the proposed protocol provides good experimental results on various metrics like throughput, end-to-end delay, and PDR. Analysis of the results points to an improvement in the overall network performance.**

Index Terms— **R-AODV, ECC, NS-2.35, Packet drop ratio (PDR), Throughput, End-to-end Delay, Blackhole Attack**

I. Introduction

Mobile Adhoc Network is a wireless communication network that consists of a set of mobile nodes that are temporarily connected without any infrastructure. A MANET is formed using wireless hosts which may be mobile, hence leading to a rapid change in topology. In MANETs, communication can be done directly for nodes within the transmission range; however, outside the range, it will rely on other intermediate nodes for transmission. The complex nature of MANETs makes the network vulnerable i.e., unstable and accessible to attacks. Routing is one of the critical elements of any network. Every node should not only function for itself but should also cooperate with the other nodes. MANETs are vulnerable to various types of security attacks. But seeking a safe and trustworthy end-to-end path in a MANET is a real challenge.

MANETs do not define a physical boundary, due to which any node is allowed to enter and leave the network as per their need. In this process, an adversary node can enter the network and begin its attack. Types of attacks are Denial of Service attack, Blackhole attack, eavesdropping, tempering, Jellyfish attack, neighbor attack, etc.

There have been numerous techniques created to increase the security of a MANET; one of the ways is to secure the data that is to be transmitted over a hostile environment so the data remains secure despite the attack. To implement the mentioned technique, we have applied the ECC algorithm along with R-AODV and have shown the impact of a Blackhole Attack on the proposed method.

To ensure secure transmission, various encryption algorithms have already been used with a myriad of protocols. However, the frail nature of certain protocols does not let the MANET keep the transmission secure for a long period. Tarandeep Kaur et al. [1] observed performance evaluation of various protocols under a Blackhole attack and concluded that protocols like Ad Hoc on-demand Routing (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) take a serious hit under an attack and their performance significantly degrades which leads to a great amount of loss in data. Harmandeep Singh et al. [2] deduced that the effect of the Blackhole attack is relatively higher on AODV when compared to other protocols. Mohan Kumar et al. [3] proposed the implementation of RSA for secure routing in the network, malicious nodes were detected since the hop count field and sequence numbers were encrypted. However, this proposal still needs to be expanded & tested for larger networks. In our proposed system, we focused on the encryption algorithm (ECC) and the implementation of R-AODV which decreases power consumption and communication delay when compared to AODV.

The rest of the paper is organized as follows: Section 2 contains the related work; Section 3 discusses the properties of the Blackhole attack, R-AODV protocol, and Elliptic Curve Cryptography (ECC), the reasons behind choosing R-AODV as the routing protocol, and ECC as encryption technique. Section 4 depicts the implementation of the system, Section 5 discusses the generated results, and lastly, section 6 portrays the conclusion and future enhancement.

II. Related Work

Some of the countering mechanisms of blackhole attack are overviewed as follows:

Jeenat Sultana et al., in “Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET” [4], proposed an approach to secure data transmission against a blackhole attack in MANETs. They implemented a prevention protocol using ECC along with the AOMDV. The encrypted

978-1-7281-9287-1/20/$31.00 ©2020 IEEE

packets that transfer between the nodes through AOMDV are secured. Using different metrics, the performance of the secured protocol has been analyzed.

Ashok Koujalagi, in "Considerable detection of blackhole attack and analyzing its performance on AODV routing protocol in MANET (Mobile Ad Hoc Network)" [5], proposed a strategy to find the blackhole attack on the AODV protocol in MANET. This technique considers that the first route reply packet that it has received is the reaction from the malicious node and, therefore, removes the intruded node from the network. And when the second route reply packet is received, it is considered for the route reply saving mechanism as it originates from the goal hub. He has named this technique as the Blackhole Detection System. The modified AODV with this BDS arrangement against node has a high packet delivery ratio when contrasted with the already existing AODV protocol under a blackhole attack.

Sushil. Kumar et al., in "Analysis and Implementation of AODV Routing Protocol against Blackhole Attack in MANET" [6], used the NS-2 network simulator to analyze the performance of AODV under a blackhole attack. It is found that the throughput of normal AODV increased with the number of nodes, but network throughput dropped drastically when the Blackhole Attack occurred. As the number of nodes increases, fewer packets are discarded by normal AODV, whereas in the case of Blackhole Attacks, the total number of dropped packets is much more than normal. Besides, the end-to-end delay of normal AODV is much longer, but the packet delivery rate of normal AODV is much higher than Blackhole Attacks.

Akhilesh Singh et al. in "An Improved Mechanism to Prevent Blackhole Attack in MANET" [7], proposed a mechanism to prevent the cooperative blackhole attack in which DSN is compared with the threshold value to discard the fake messages. NS2 network simulator is used to analyze the performance of the proposed approach based on PDR.

Guoquam Li et al., in "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network" [8], designed blackhole attack scenarios in AODV to study the impact of Blackhole Attack on network performance parameters, using the NS-3 network simulator. Changes in the network performance and movement speed of mobile nodes are analyzed by adjusting the number of blackhole nodes and the total they studied various security issues in and the behavior of blackhole attack.

Mohammed Imran et al., in "Detection and Prevention of Blackhole Attacks in Mobile Ad hoc Networks" [9], proposed a Detection and Prevention system (DPS) to detect a blackhole attack in MANET. These DPS nodes are deployed in the network which monitors RREEQs broadcasted by the other nodes. DPS nodes observe the behavior of the nodes and detect the malicious activity in the network and then it declares it as a suspicious blackhole node. Therefore, the blackhole node is isolated from the network, and no data is passed to it. The simulation is done using the NS-2 simulator which shows the reduced packet drop ratio with a low false-positive rate.

III. Methodology

A. *Blackhole Attack*

In a Blackhole attack, a malicious node promotes itself to have the shortest path in the entire network to the destination node. This node publicizes its availability of fresh routes regardless of it having any or checking its routing table. Consequently, all the packets end up passing through the malicious node, due to the cooperative nature of MANETs. Like all the normal nodes in MANET trust every reply they get for their broadcasted request over the network, the malicious node takes an advantage of this flaw and exploits it. The blackhole node ends up dropping packets instead of forwarding them to the destination node.

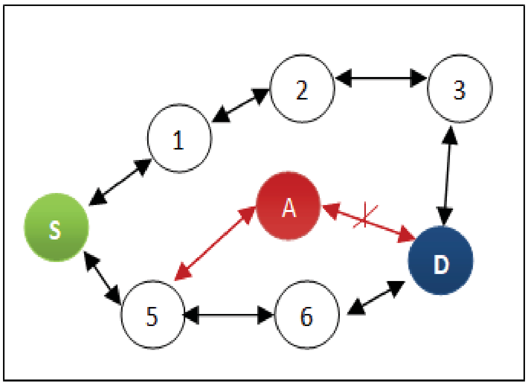


Fig. 1. Demonstration of a Blackhole attack in a MANET

Figure 1, depicts an example of how a MANET functions in the presence of a Blackhole (BH) attack. Here, node A is the malicious blackhole node. The node S which is the source node initiates the route discovery process and determines the path to the destination node D by broadcasting the RREQ (Route Request) messages and then begins forwarding the data packets. Node A which is a blackhole node produces bogus RREP (Route Reply) packets while processing RREQ packets with a smaller hop count. Upon receiving the RREP packet, the source node begins the data transfer to forward the data packets to the blackhole node thinking that it is the destination node. The blackhole drops all the data packets instead of transmitting it to the other node. Therefore, node D will not receive any data packet.

B. *Reverse Adhoc On-demand Distance Vector (R-AODV)*

MANET is formed using wireless hosts which may be mobile, hence leading to a rapid change of topology. Most of the reactive routing protocols, except for multipath routing, use a single route reply along the first reverse path. The source node has to retransmit route request messages, as pre-determined reverse paths can be disconnected and route reply messages from destination to source can be skipped in high mobility. R-AODV aims to improve the possibility of creating a route with fewer RREQ messages than other protocols. Routes are explored utilizing the R-AODV reverse route discovery procedure. Both the source node and the destination node play the same function in sending control messages throughout the route discovery procedure. To reach the source node, the destination node floods with a reverse request (R-RREQ) then the data packet transmission begins after the source node receives an R-RREQ message [10].

There are no permanent routes stored in the nodes, in the reactive routing protocol. Figure 2, shows the flowchart for route discovery using R-AODV. The route discovery process is initiated only after the source node broadcasts the RREQ packets in the network. Whenever a new RREQ is issued, the broadcast ID is incremented by one. The source and destination node identify the unique RREQ packet. The data packets are then forwarded by the intermediate nodes to other nodes in the same manner. The redundant RREQ messages that are forwarded by the nodes are dropped. The destination node generates a reverse request message (R-RREQ) as soon as it receives the first route request message and then broadcasts it to the neighboring nodes. As soon the source node receives the first R-RREQ message the data packet transmission is initiated and the late arrived packets are saved for future use.

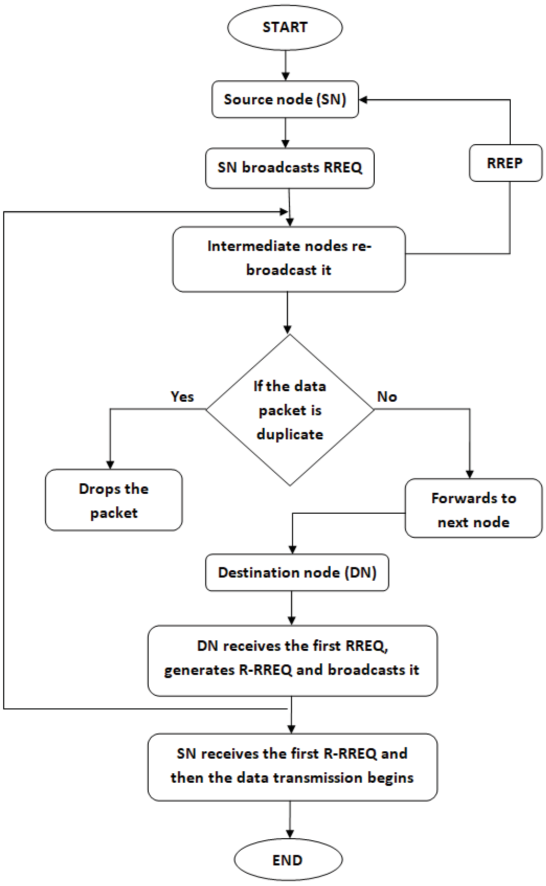

START
Source node (SN)
SN broadcasts RREQ
RREP
Intermediate nodes re-broadcast it
If the data packet is duplicate
Yes
No
Drops the packet
Forwards to next node
Destination node (DN)
DN receives the first RREQ, generates R-RREQ and broadcasts it
SN receives the first R-RREQ and then the data transmission begins
END

Fig. 2. Flowchart for the route discovery using R-AODV

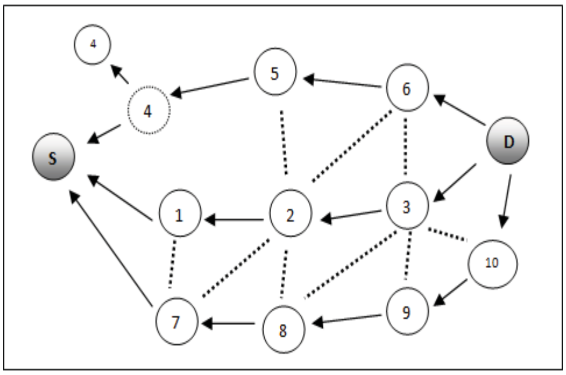


Fig. 3. R-RREQ from Destination to Source Node

In Figure 3, of R-AODV, the destination does not unicast reply along with pre-decided shortest reverse route D → 6 → 5 → 4 → S. Rather, it floods R-RREQ to find source node S. And forwarding path to the destination is built through this R-RREQ. The following paths may be built: S → 1→ 2 → 3 → D; S → 7 → 8 → 9 → 10 → D; and so on. Node S selects the best path and starts forwarding the data packet. So the RREP delivery fail problem does not occur in this case, even though node 4 moves from the transmission range.

C. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography is used to provide secure transmission. Elliptic curve cryptosystems are based on the Discrete Logarithm Problem. ECC is a method of maintaining encryption from shorter keys and has the same protection standard as RSA i.e., ECC has a high-security level with a smaller key size. The security of ECC is mainly due to the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). So the attacks over ECC try to solve the ECDLP problem. The main advantage of ECC is its high-security level with a smaller key size [11]. Thus with ECC, it will be tough for the blackhole attacker node to retrieve the private key from the given secret key and public key.

Figure 4, shows the encryption and decryption process by ECC. The source node generates a public/private key pair. Initially, a random private key is chosen and a secret key is generated from its private key and the receiver's public key. The encryption of the packet is done using the freshly generated secret key and announces the public key and sends it via R-AODV protocol. The destination node generates the same secret key with the help of its private key and the sender's new public key, after receiving the encrypted packet. Then the receiver decrypts the packet to get back the original data using its shared secret key and public/private key pair. Thus, without the shared keys, the malicious node can't decrypt the data.

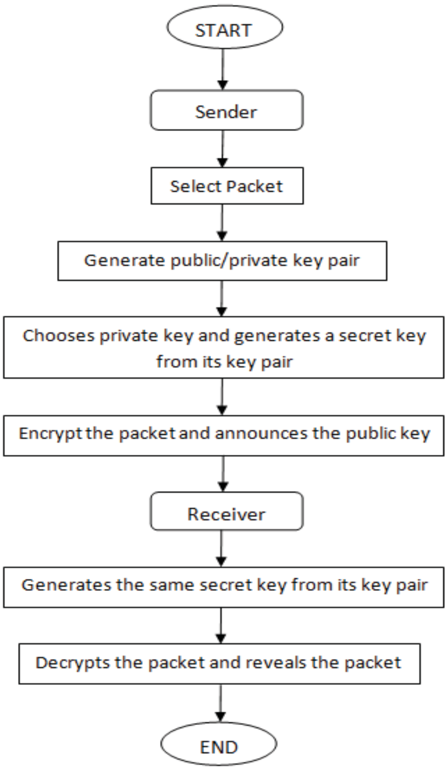

START
Sender
Select Packet
Generate public/private key pair
Chooses private key and generates a secret key from its key pair
Encrypt the packet and announces the public key
Receiver
Generates the same secret key from its key pair
Decrypts the packet and reveals the packet
END

Fig. 4. Packet encryption/decryption by ECC

D. Problem Statement

Security of MANET is essential to prevent the harm that could be caused by the blackhole attack. The blackhole attack is considered to be one of the most popular attacks that harm the network and works on preventing any sort of communication or connection in the network. To increase security, an ECC approach is used with its complicated logarithmic concern with the use of R-AODV to replace the flaws of AODV, which is one of the most preferred protocols for a MANET. With both ECC and R-AODV being used together we aim to increase the security, performance, and consistency of the network and to put forward an efficient prevention and avoidance mechanism against it.

E. Proposed System

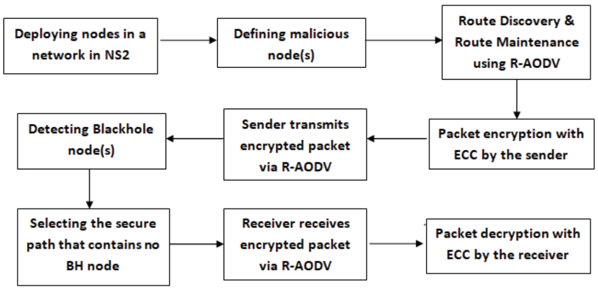

Deploying nodes in a network in NS2
Defining malicious node(s)
Route Discovery & Route Maintenance using R-AODV
Packet encryption with ECC by the sender
Sender transmits encrypted packet via R-AODV
Detecting Blackhole node(s)
Selecting the secure path that contains no BH node
Receiver receives encrypted packet via R-AODV
Packet decryption with ECC by the receiver

Fig. 5. Block diagram of the proposed methodology

Figure 5, shows a sequence of steps to secure the data packets in MANETs which contains a blackhole node. Initially, a topology is established and nodes are deployed on the network. Then the malicious node(s) will be defined. The route discovery process via R-AODV protocol takes place where all the feasible routes between the source and the destination are discovered. If the route fails, then the other route will be ready to take its place and starts data transmission. With the help of ECC, keys are distributed among the valid nodes in the MANET, and data encryption as well as data decryption process occurs. This is done by using public/private keys. Furthermore, the data will securely be transmitted between the two main nodes without having to worry about the packet loss, as it will be tough for the malicious node to reveal the original data without the shared secret keys. The data is securely transmitted to the destination node, using the path which does not contain blackhole node. It will be difficult for the blackhole node to open and read the data packets.

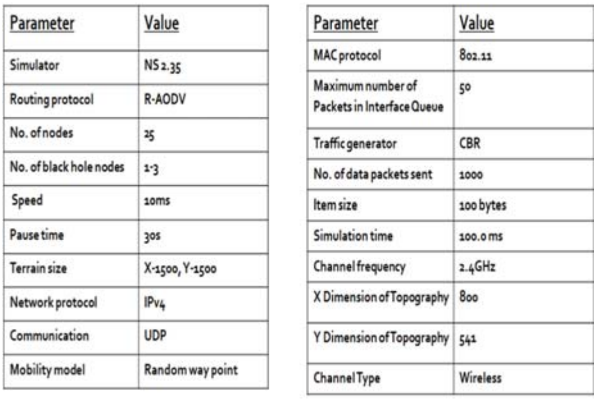
F. Algorithm

```
Steps:
1.  Topology formation
2.  Establishing the source, destination, and attacker node.
3.  Set up traffic generators, viz. CBR connections.
4.  Route discovery by R-AODV by broadcasting RREQ from
    source to destination
5.  RREP's are unicasted back to the source
6.  Routing tables are created or updated (noting the sequence
    number and hop counts of the nodes)
7.  Initiate data packet transmission
8.  The sender encrypts the data using ECC
      //Check for the presence of malicious node
      if the Blackhole node is detected then
              block the node and choose a different path
      else
              forward the data packet to the next node
      end
9.  The receiver decrypts the data using ECC to get back the
    original data packet
```

IV. System Implementation

Network simulator (NS2) is a discrete-event simulator used to study the vibrant nature of MANETs. In this paper, the NS-2.35 simulator is used for simulation of the proposed system. The area considered is 800 x 541 meters and the wireless topology contains 25 nodes that include one blackhole node. Communication between the nodes is done using UDP. The total time used for simulation is 50 seconds the simulation scenario is shown in table 1.

TABLE 1
SIMULATION ENVIRONMENT



Parameter	Value
Simulator	NS2.35
Routing protocol	R-AODV
No. of nodes	25
No. of black hole nodes	1-3
Speed	10ms
Pause time	30s
Terrain size	X-1500, Y-1500
Network protocol	IPv4
Communication	UDP
Mobility model	Random way point

Parameter	Value
MAC protocol	802.11
Maximum number of Packets in Interface Queue	50
Traffic generator	CBR
No. of data packets sent	1000
Item size	100 bytes
Simulation time	100.0 ms
Channel frequency	2.4GHz
X Dimension of Topography	800
Y Dimension of Topography	541
Channel Type	Wireless

A sub-network architecture involving 25 nodes is modeled with IPv4 and IPv6 as depicted in Figure 6. A CBR traffic from the originator to the target is triggered, channeling 1000 packets all of magnitude 100 bytes. The time of the simulation is maintained to be 100 seconds. Source node, Destination node, Blackhole node are set as node 1, node 3, node 24 respectively. The framework first implements the attack module that uses the Blackhole node 24 to reroute the packets from the source to itself by suggesting an optimal path and then discards it. The prevention module then subsequently discovers the attack and uses the other optimal route that it had previously stored to send the packets. The behavior of the network is then explored and analyzed.

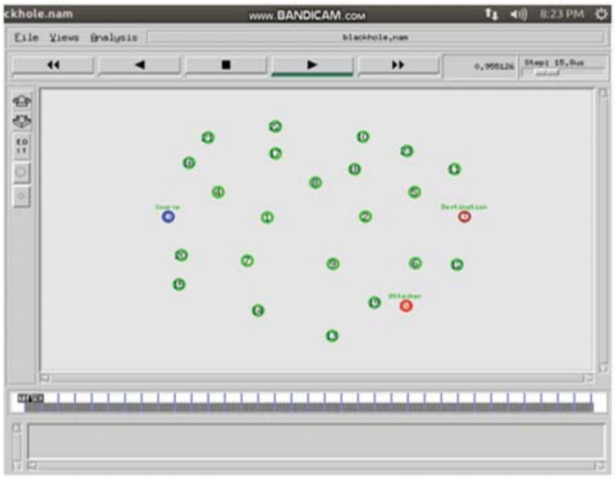


Fig. 6. MANET consisting of 25 nodes

V. EXPERIMENTAL RESULTS

End to End delay:

Average transmission delay is the average amount of time utilized by a data packet to shift from initiator to the target end. Average transmission delay(s) = aggregate bits / transmission rate (bits/sec).

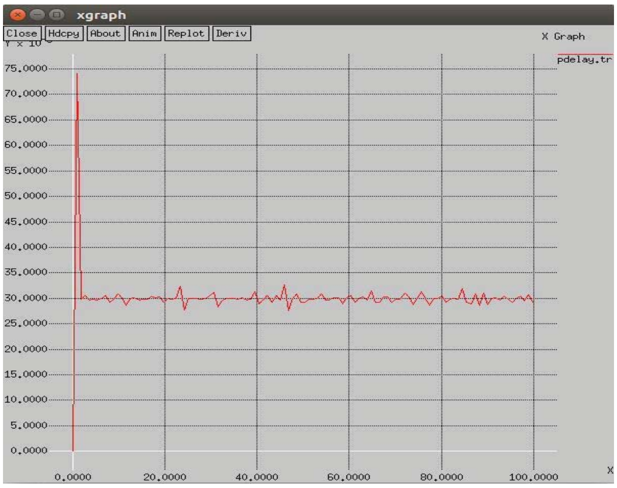


Fig. 7. Delay- on using prevention protocol

The X-graph showed in Figure 7, displays the study of the average transmission delay. In the absence of the spiteful attack, the transmission delay is optimal and it can be perceived that the delay is high in the presence of the attacking nodes in the network. With the applied prevention plan this influence is curtailed.

Packet Drop Ratio:

The packet loss rate is the difference between the packets received and the packets transmitted.
Packet drop ratio= (No. of packets gained – No. of packets dispatched) *100.

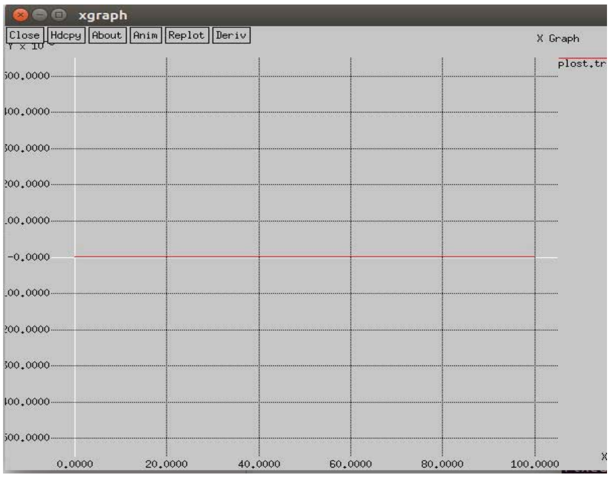


Fig. 8. Packet loss – on using prevention protocol

The packet loss rate in the absence of malicious nodes is insignificant, whereas after the spiteful nodes are implanted the packet loss has shot up enormously thereby striking at the network performance. With the prevention, the packet loss was successfully lowered to 0 as can be seen in Figure 8.

Throughput:

Throughput is the aggregate of packets dispatched per unit time.

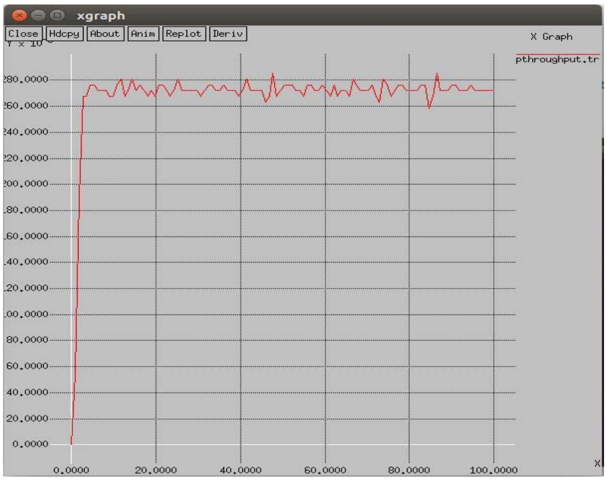


Fig. 9. Throughput – on using prevention protocol

After the prevention, the throughput values are found to be optimum with a negligible difference. By inspecting the throughput against time we can note that the proposal is practically effective to prevail over the blackhole attack. By implementing the proposal, the throughput of the network is amplified and is perceived to be very close to the throughput in the normal conditions as depicted in Figure 9.

Comparative analysis of the different parameters used:

The base paper [4] is taken into consideration as the existing system for comparing the results generated in the presence of blackhole and after using the proposed prevention protocol.

The abbreviations used in the graph are as follows:

BH = in the presence of blackhole attack
ES = existing system
PREV = prevention protocol

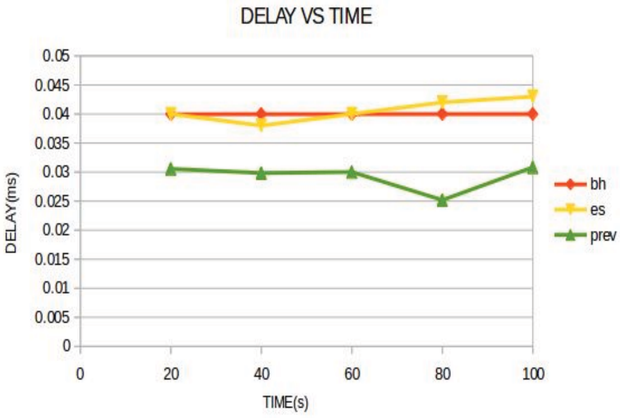


Fig. 10. Delay vs. time

Figure 10, shows the comparison of the delay for the attack, prevention, and the existing system. The delay for the existing system and in the presence of a blackhole attack is almost the same around 40 ms but after applying the proposed methodology it decreases a bit to 30 ms. In the absence of the spiteful attack, the transmission delay is optimal and it can be perceived that the delay is high in the presence of the attacking nodes in the network. With the applied prevention plan this influence is curtailed.

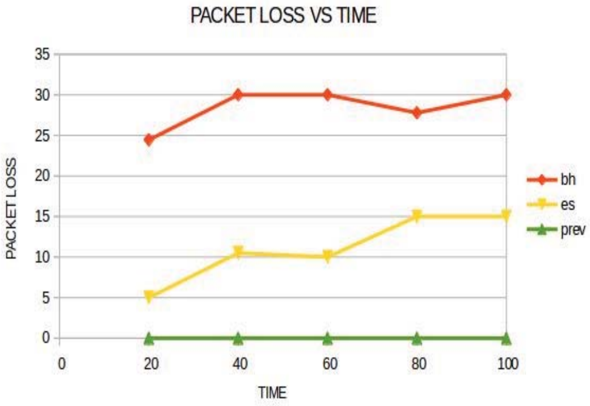


Fig. 11. Packet drop ratio vs. time

Figure 11, shows the packet loss ratio observed in the existing system, blackhole attack, and the proposed system. The packet drop kept increasing in the presence of a blackhole node in MANET. But when the proposed method is implemented, then in the presence of a blackhole attack node being present in the network, there is no packet drop in the network. With the prevention, the packet loss was successfully lowered to 0.

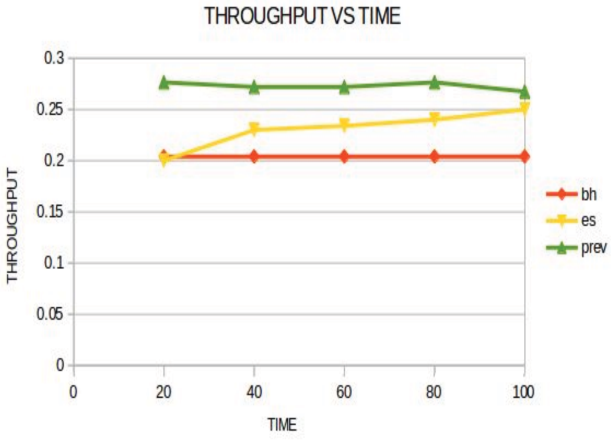


Fig. 12. Throughput vs. time

Figure 12, shows the comparison of throughput for attack and prevention with the existing system. The result shows that the throughput generated in the presence of blackhole (200 kbps) is lesser (it has dropped) compared to the throughput generated in the existing system (which rising to nearly 270kbps). But with ECC implementation in prevention R-AODV protocol, the value is increased to 290 kbps. By inspecting the throughput against time we can note that the proposal is practically effective to prevail over the black hole attack. By implementing the proposal, the throughput of the network is amplified and is perceived to be very close to the throughput in the normal conditions.

VI. Conclusion And Future Enhancement

The aim of the proposal is to secure the data packets and deliver them successfully to the destination node without data being transmitted to the attacker. The proposed approach uses ECC along with R-AODV for the improvement of security between the nodes and to enhance the data transfer performance in the MANET environment. It detects and prevents the malicious behavior of the node through the R-AODV route discovery process, which succeeds in fewer tries than on-demand routing protocols. The performance is evaluated using the NS-2.35 network simulator and provides good experimental results on different parameters like throughput, delay, and packet loss. The method can be implemented along with an intrusion detection system (IDS) to detect and to avoid malicious node.

References

[1] Tarandeep Kaur and Amarvir Singh, "Performance Evaluation of MANET with Blackhole Attack Using Routing Protocols", International Journal of Engineering Research and Applications (IJERA), 2013, Vol. 3, No. 4, pp. 1324-1328.

[2] Harmandeep Singh, Manpreeet Singh, "Effect of Blackhole Attack on AODV, OLSR and ZRP Protocol in MANETs", International Journal of Advanced Trends in Computer Science and Engineering, May – June 2013, Vol. 2, No. 3, ISSN: 2278-3091.

[3] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", International Journal of Computational Engineering & Management (IJCEM), 2011, Vol. 11, ISSN: 2230-7893.

[4] Jeenat Sultana and Tasnuva Ahmed, "Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET", International Journal of Electrical and Computer Engineering (IJECE), December 2018, Vol. 8, No. 6, pp. 4412-4422, ISSN: 2088-8708.

[5] Ashok Koujalagi, "Considerable detection of blackhole attack and analyzing its performance on AODV routing protocol in MANET (Mobile Ad Hoc Network)", American Journal of Computer Science and Information Technology, 2018, Vol. 6, No.2:25, ISSN: 2349-3917.

[6] Sushil. Kumar, Deepak Singh Rana and Sushil Chandra Dimri, "Analysis and Implementation of AODV Routing Protocol against Blackhole Attack in MANET", International Journal of Computer Applications, 2015, Vol. 124, No. 1, ISSN: 0975-8887.

[7] Akhilesh Singh and Muzammil Hasan, "An Improved Mechanism to Prevent Blackhole Attack in MANET", Progress in Advanced Computing and Intelligent Engineering, 2018, Vol 563, pp 511-520.

[8] Guoquam Li, Zheng Yan and Yulong Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network", IEEE Conference on Communications and Network Security (CNS), 2018, pp. 1-6.

[9] Mohammed Imran, Farrukh Aslam Khan, Haider Abbas and Mohsin Iftikhar, "Detection and Prevention of Blackhole Attacks in Mobile Ad hoc Networks", Garcia Pineda et al. (Eds.): ADHOC-NOW Workshops 2014, 2015, LNCS 8629, pp. 111–122.

[10] Choggun Kim, ElmurodTalipov, and ByoungchulAhn, "A reverse AODV Routing Protocol in Ad hoc Mobile Networks", X. Zhou et al. (Eds.): EUC Workshops 2006, 2006, LNCS 4097, pp. 522- 531.

[11] K.Sangeetha, "Secure Data Transmission in MANETS Using Elliptic Curve Cryptography", International Journal of Innovative Research in Computer and Communication Engineering, March 2014, Vol. 2, No. 1.