Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 7, Issue 03, March -2020

Implementation of Security in IOT-MANET Networks

Yousaf Ali[1], Dr. S.M Majid Ashraf[2]

Research Scholar Department of Electrical Engineering University of Engineering and Technology Peshawar

[2] *Assistant Professor Department of Electrical Engineering University of Engineering and Technology Peshawar*

Abstract: *In this Research work we have implemented the encryption technique to secure an Internet of Things based network with Mobile Ad-hoc network nodes against the network layer attack. With a very large number of nodes, sensors and other devices in internet of things has created security challenges for network engineers and researchers, the node mobility of MANETs have increased the vulnerability if IOT-MANETs network. We have consider the black hole attack as our network layer attack and modified the Ad-hos on Demand Distance Vector routing protocol to mitigate the black hole attack. The RSA encryption technique is used to encrypt and decrypt the routing messages. Two keys are used, the public key and private key. Public key is used to encrypt the route request messages while the private key is used to decrypt these messages. The research work is implemented in the network simulator-2. Results of simulation are compared in the performance analysis section.*

Keywords*: Internet of things, IoTsecurity mobile ad-hoc network, black hole attack, ad-hoc on demand distance vector protocol, RSA encryption.*

I. INTRODUCTION

Internet of Things (IOT) is the interconnection of devices, apparatus and appliances at home, industries, Power houses and educational Institutes through internet. The devices are controlled remotely via internet with the help of sensors. Internet of things is changing life of humans and making it more comfortable. Internet of things communication takes place with a set of predefined model and protocol. Security in the Internet of things is of great importance because of wide variety of devices, sensor and computers used in the environment [1]. The Internet of things communication takes place on four layers; the Perceptual layer, Support layer, Network layer and Application layer. In this work we have used mobile ad-hoc network node so let us have a look at Manet network. The MANET (Mobile ad-hoc network) is a type of wireless networks that are self-organizing and auto connected in a de-centralized system. Every node in MANET can be moved from one place to another in any direction. They can makes a network with their neighbors' nodes and forward data to another nodes. The MANET uses the ad-hoc routing protocols such as AODV,DSR and DSDV etc. In this research we will considering the widely used routing protocol AODV Ad-hoc On Demand Distance Vector routing protocol which is widely used because it is proactive and energy efficient routing protocol.

II. RELATED WORKS:

Several principles have been presented to improve and boost the efficiency and security of IOT-MANET in the AODV protocol. In [2] the author proposed the employing of timers and baiting messages technique. It was composed of two steps the baiting and neighbor reply.in baiting the every node has a bait timer with timer value randomly selected to a certain value. Each time the timer value reaches the certain fixed value it created the bait request with randomly generated fake id. When the black hole attack node receives this request it will generate the route reply message saying it has the route to the destination and send route reply to source. After getting reply from black hole attack node the source will add the attacker node to the list of black hole attack node and will avoid this node in future. In [3] the author has proposed the black hole isolation technique where he used the fake route request message as a tool to detect the attacker node, the source node will send fake route request message to all network node. No healthy node will respond to this node because they do not have route to the fake destination address, while receiving this request the black hole attack node will respond will reply message. The source node after receiving the route reply from black hole attack node will detect and isolate the malicious node from network. In [4] the solution to this kind of attack was proposed as the enhanced AODV routing protocol. It suggested that the RREP message must be monitored along with the history. It adds the address of last node which has route to destination. They added two tables one is suspect table while the other is blacklist table. Suspect table has address of all node from which they received the route reply message while those from which the route reply are not received are placed in black list table. All messages arrived from the black list table node will be ignored. In [5] Chaudhry proposed that each node in the network must use a maximum trust value when the source node send the route request messages the the first neighbor will reply with RREP message according to this method when N node send R-REQ message and N+1 node respond with RREP message it set the time in seconds when it expires the source start hearing form medium to see if it has received the same data it sent to

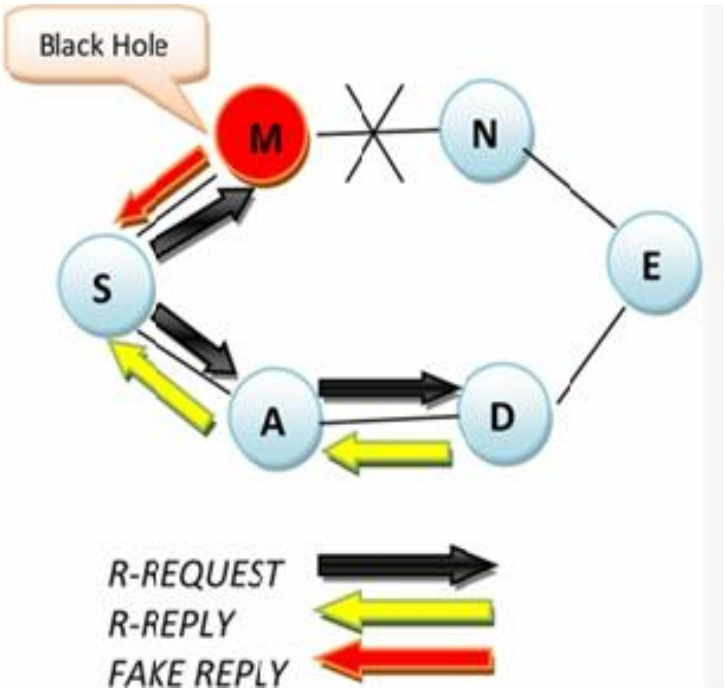
the N+1.if I did not received any thing it will decreas the trust value of N+1 by 1. This information is propagated. When the trust value become less than the threshold valueas pre-defined, the node will be black listed and all the messages coming from this node are ignored and the node is remembered as malicious node.

III-A**DOS ATTACK**

Denail of Service (DOS) attack is a network -attack whereby the attacker intrude in to the computer or network and make the resources or services unavailable for the authorized users. This attack is accomplished generally by flooding the computer or a network device with multiple request and thereby overburdening the resource or device to be available for other users. If the flooding request messages are coming form multiple sources this DoS attack will be called as distributed denial of dervice attack (DDoS). Dos and DDoS attack is like overcrowding the grocery shop to make it unable for buyers to purchase the goods.

III-B**BLACK HOLE ATTACK**

Black hole attack is network layer attack of Denial of Service attack, This attack take place when the routers or node initiate the route discovery process to update and maintain the routing table. When a router is intended to send the data to a specific destination it will ask for the most suitable route from all the neighbor the request is send for route discovery this request is called as route request message RREQ. The neighbor routers when receive the RREQ reply with the route reply if the route is available within its routing table called as RREP message. If the path is not available within the routing table it will forward the request to further nodes to find for suitable path.In black hole attack when the malicious node receive the RREQ message it do not check the path to the destination in its routing table nor it forward to further neighbors but will directly reply to the source node that I have to shortest and suitable path to the destination. So upon receiving this reply the source start sending data to this attacking node called as black hole attack node, The black hole attack node then destroy the data packet. The process is explained the figure below, the node **S** is source node, **D** is destination node and **M** is the black hole attack node.



III-C**AODV ROUTING PROTOCOL** The Ad-hoc on demand distance Vector protocol is a dynamic routing protocol developed by Nokia Research Center at California for Mobile adhoc networks back in 2003. AODV is low power and low data rate protocol suited for mobile nodes. AODV protocol is used in IOT-MANETs combination of networks. In AODV routing protocol the source and destination IP address are already known, the goal is to find the ideal and low cost route to the destination from the source and to maintain the route, The AODV routing table is made and maintained with certain messages called as RREQ,RREP route request and route response respectively [5]. RREQ is initiated by the source node to

ask for the route to the destination and RREP route response is the reply of neighbor and destination node to the previous node giving information about the route to destination. The format of RREQ and RREP is

RREQ{Source IP address, Destiation IP Address, Hop Count,SourceSequence Number,Destination Sequence Number}

RRES{Destination IP Address, Destination Sequence Number,Source IP Address,Life Time}.

III-D **RSA SECURED ROUTING** We will explain how RSA algorithm will be used to secure the MANET nodes in IOT from Black-hole attacks. Since the black hole attack takes place at first stage of routing process i-e the routing discovery [6]. The black hole nodes when receive the RREQ packets from the source node immediately sends the fake replies to source about the route to destination. This way the source start sending data packets to black hole node and which are destroyed by this malicious node [7]. So to prevent this attack we will apply the RSA encryption technique on route discovery packets.

The Following steps will explain how the RSA will secure the routing process and prevent the fake route replies from balckhole node thereby preventing black hole attack.

Step1- Calculate the Public and private keys using the RSA technique explained earlier, let e and d are the public and private keys respectively.

Step2- Generate the RREQ message and encrypt it using the Public key e as;

for (inti=0; i<e; i++)

C is Encrypted text which is C=1 initially

C=C*M mod n

Where M is original RREQ packet.

Step3- The encrypted RREQ packet is forwarded from source to all neighbors nodes.

Step4- If the receiving node is not a black hole node the decryption will take place using the private key d.

for(i=0;1<d;i++)

M = M*C mod n

M is original message obtained after encrypting the Encrypted message C with private Key d.

Step5- If the RREQ is received by black hole node it will create the fake RRES reply and send to source.

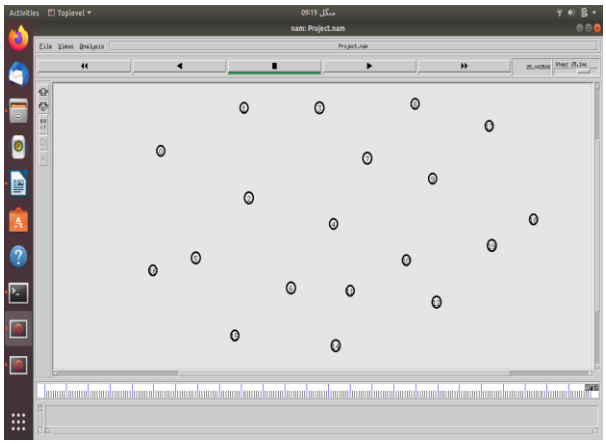
Step6- If the RRES is from black hole node, the RRES will not be encrypted correctly and the corresponding flag will be set showing that the reply is from black hole node and source will ignore this RRES message.

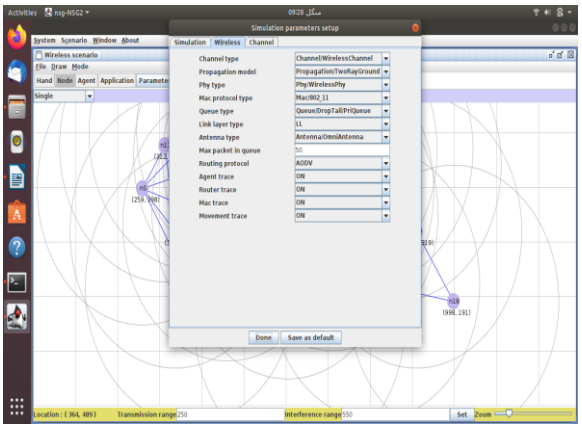
Step7- If the RRES is from non-malicious node, the RRES will be encrypted correctly and the corresponding flag will be set showing that the reply is from non-malicious node and source will establish the path and update the routing table.

IV- **SIMULATION SETUP**

We used Network Simulator-2 model NS-2.35 for simulating our network and applying the RSA security algorithm for securing our IOT-MANET network from black hole attack, the routing protocol used is AODV protocol.

The network consist of 20 Nodes, the node 0 is the source node while the node 12 is the destination node. The node 2 is configured to be the black hole attack node. The black hole node will take the packet from source and destroy it instead of sending it to destination.

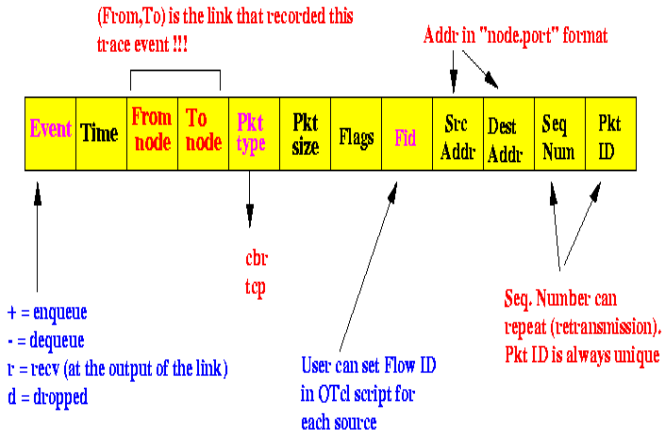


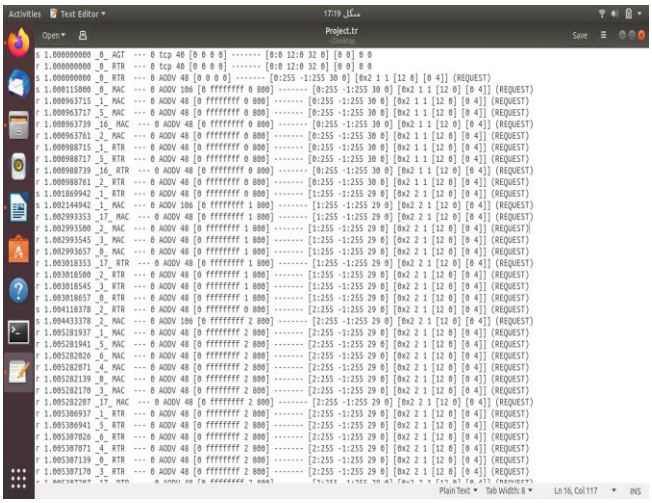


V-**TESTING THE SYSTEM**

The Network Animation files are used to run and simulate the system with all healthy nodes, with a black hole node and with RSA secured mechanism to prevent the attack. The three simulations and their results are compared using the NAM and different graphic tools, the packet transmitted, received and drop are calculated and compared for all of the three cases.

Trace file are further used to monitor and calculate the packets transmitted between node, format of trace file is given in the figure below.





VI- **EXPERIMENTATION AND RESULTS**

THE PACKET DELIVERY RATIO

Noted **(PDR)** the ratio of all the packet received at receiver to the sum of all packet sent by the sender. PDR gives us the processing and data transfer ability, and main parameter of effectiveness, integrity, reliability and correctness of the method. High Packet delivery ratio means the network and the used protocols are performing well. The following equation calculate the packet delivery ratio of the network

PDR = Sum of all Packets received /Sum of all Packets sent ∗100 %

Result of three type of networks are shown below, a healthy network, black hole attack network and RSA secured network.

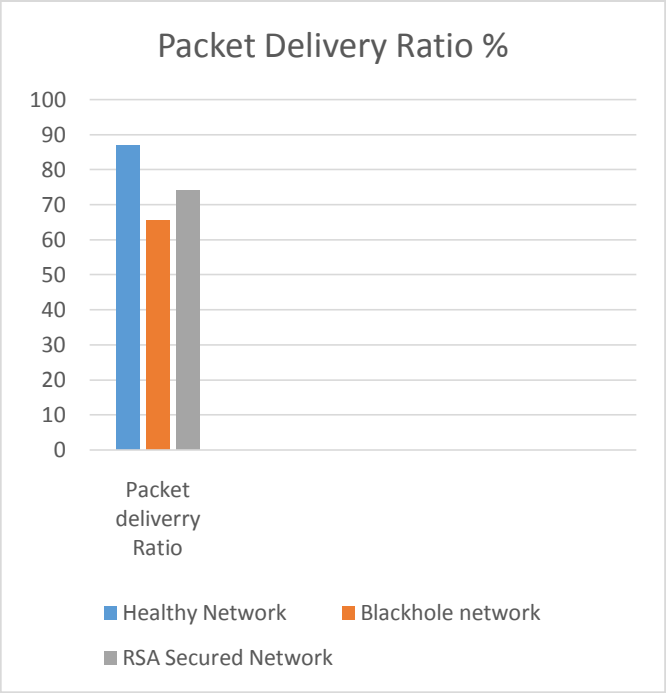
THROUGHPUT

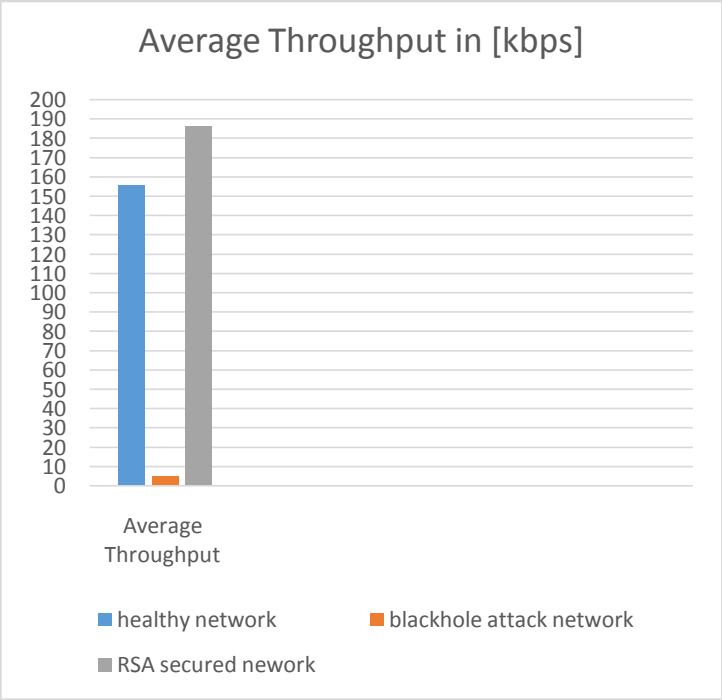
It is the sum of all data packets received by destination in a unit time.

The following equation is used to calculate the throughput of network.

Throughput = Sum of Size of received packets/ Sum of (Stop Time- Start Time)

Result of three type of networks are shown below, a healthy network, black hole attack network and RSA secured network.





VII-CONCLUSION

Security is one of the key aspect of any network, same is the case with IOT-MANET networks with evolution of 5G communication it is the hot research topic to secure the IOT of different attacks. In this work we focused on one of the network layer attack on IOT-MANET attack namely blackhole attack. The attacker node send fake route replies to source node that I have the shortest and cost effective path to the destination and thereby start receiving data packets from the source and destroy it. We have used the RSA algorithm to secure network from this kind of attack by encrypting the route discovery packets and encrypting route response message. Encryption is done with public key while decryption is done with private key, only healthy nodes have private key so attacker node were not able to decrypt the route messages and therefore the destination did not considered the replies from the attacker black hole node. The RSA algorithm were implemented in Network simulator-2. The result of the three case, one with all healthy node, with black hole node and RSA implemented network are compared and graphs and table are drawn.

VIII- REFERENCES

[1] Beyond the Internet of Things", Springer Science and Business Media LLC, 2017
[2] AdwanYasin , Muhammad Abu Zant “Detecting and isolation of black hole attacks in MANET using timer based baited technique” Wireless communication and mobile computing by Hindawi and Wily volume 2018, 06 Sep 2018[3] Rao Sidhartha “Two step verification of isolation of black hole attack nodes” International Journal of Recent Technology and Engineering. Volume 8, Issue 4, Nov 2019.
[4] MuneerBaniYassein, Ismail Hameidi “black hole attack security issue” international conference on computer science at Dubai UAE, 2018. [5] Chaudhry N “Preventing blackhole attack in Manet“ International Conference on SPACE IEEE” Jan 2015.
[6] Ahmad Alomari. "Chapter 48 Security Authentication of AODV Protocols in MANETs", Springer Science and Business Media LLC, 2013.
[7] Deepadasarathan, P. Nirmal Kumar. "A novel method to avoid stale route cache problem of dynamic source routing protocol for mobile ad hoc network", 2013 International Conference on Current Trends in Engineering and Technology(ICCTET), 2013.

