IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 1, Ver. II (Jan. - Feb .2016), PP 35-39
www.iosrjournals.org

A Review Paper on Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's

T. Gopala Krishna[1], R .Jaya Lakshmi[2], K. Umapathy[3],
[1]*Mtech Edt*
[2]*Assistant Professor*
[3]*Associate Professor*
Department Of Electronics And Communication Scsvmv University , Kanchipuram

Abstract*: Networks are being used in various areas of mobile ad-hoc network (MANET) used in network in Laptops, and smart phones. A mobile ad-hoc network (MANET) is a continuously self-configuring, infrastructure with less network of mobile devices connected with out wires .MANETs are a kind of wireless ad-hoc network that usually has a routable network environment MANET consists of a peer-to-peer, self-forming, healing network . In MANET several routing protocols are used AODV is the one among the routing protocols and it has the different characteristics because it has reactive routing Protocol and it overcomes the disadvantages of DSDV routing protocol. When the error message is sends back to Source and the procedure gets repeated, the failure of the link will degrade its characteristic .we are proposing a method when links or nodes fail to receive the data packets.RC6 is the cryptographic technique is used to secure the network*
Keywords*: cryptography, mobile ad-hoc network, NS2, RC6, Routing protocol and Security.*

I. Introduction

Adhoc networks came into existence when more than two wireless mobile nodes accepts to pass packets to each other .In MANET, [AODV] Adhoc on Demand Distance Vector routing protocol is frequently used. Popularity, on networking motivated the development of adhoc mobile networks .Adhoc mobile network is a continuously self-configuring ,infrastructure-less network connected to mobile devices with out wires .Adhoc in Latin means 'for this'. MANETs are a kind of wireless Adhoc is a routable network environment on top of the link layer ad hoc network .MANETs consists of a peer-to-peer ,self-forming, self-healing networks.
MANETs communicate at radio frequencies (30MHz-5GHz).different attacks possible on AODV will be analyzed. Normal performance of AODV is improved .We are proposing an extended version for securing the AODV protocol and the routing protocols are studied for working of AODV.

In this paper we are going to decide evaluation parameters and attack analysis shall be done .Cryptography based security solution provided

The analysis of algorithm in terms of decided evaluation parameters will be performed. By using cryptography technique AODVs security with Network performance improved. Network simulator NS2 checks the performance factor and security factor .It is based on two languages , they are OTCL (object oriented extended version of TCL) which is a tool command language and C++.This TCL generates two files that is Trace file, Nam file. Nam file consists of network animator and Trace file consists of the information about the packets sent and packets received, timing Information The awk script calculates the packet delivery ratio , throughput ,energy, delay. In cryptography, RC6 is a symmetric key.RC6 has A block size of 128 bits and supports key sizes of 128,192, and 256 bits.

If some attack, attacks the AODV, then the evaluation parameters like PDR, throughput, delay , and energy get affected .

Various Attacks Are Given Below
A Types of Attacks
External Network Attacks

Connecting a network with an external network, especially the Internet, open a world of opportunities to internal users, Who can benefit from higher connectivity and faster information –sharing , as well as to who are interested in gaining .Access to the network for their malicious activities. External network attacks are often made possible by an insufficient internet or External security .These attacks are normally conducted by opponent who cannot gain access to the on site network hardware And rely on weaknesses in the security that a network uses to protect itself from the outside world.

Internal Attacks

An internal attack occurs when an individual or a group with in organization seeks to damage the operations or exploit Organizational assets. In many cases the attacker employ a amount of significant resources,

tools and skills to launch a sophisticated Computer attack and potentially remove any evidence of that attack as well.

1. Impersonation

This is the most severe attacks. The attacker can act as a innocent node and join the network in the type of attack. This type of Nodes join the network, they gain the full control of network and conduct distructive behavior. They spread fake routing information and they also gain access to a confidential
in three information. A network can be unprotected to such attacks if it does not employ a proper authentication mechanism .

2. Denial Of Service [DOS] :

DOS attack is an attempt to make a machine or network resource unavailable for the intended users temporarily Or indefinitely interrupt or suspend services of a host connected to the internet. A Distributed Denial of Service (DDOS) will attack the source in more than one and often thousands of unique IP addresses.

3. Eaves Dropping

Eaves dropping is secretly listening to the private conversation of others with out their concern, this is commonly thought to be unethical and there is that "eave droppers rarely hear anything good to themselves, eave droppers will always try to listen to the matters that concern them " .

4 .Black Hole Attack

Some time in AODV if in RREP the next hope information is also asked than harmful node as the next hope ,so when Confirmed with the next hope then next harmful node will reply as I am having route to the destination node but actually They don't have any information of routes to destination.
Black hole Attack Detection

In this Algorithm this idea is used for monitoring the flow of traffic. In this Algorithm nodes are divided parts
1.Regular Node: Low power and low power transmission range , not trust worthy.
2 .Back bone node: Have high transmission range and form a core that monitors the nodes
3 .Back bone core node : These nodes can be elevated to BN nodes for increasing connectivity and coverage of the network.

5. Worm Hole Attack:

Worm hole nodes fake a route that is shorter than the original one within the network this Can confuse routing mechanism which depend on the knowledge about distance between nodes.$ It has one or more malicious nodes and tunnel between them. Attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally. A launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms.

6. Sybil Attack

In this attack, a particular node in the network will have several different fake identities which have created by them .in this way it helps the malicious node to gain more specified information about the network. The validness of tolerant schemes fault is like a multipath topology in routing ,distributed storage , maintenance has a great decrease.

B . Cryptography

Cryptography includes techniques such as micro dots, merging words with images are the other ways to hide information in storage or transit. However ,in today's computer's centric world, cryptography is the most often associated with scrambling, sometimes referred to as cipher text process called encryption ,then back again called decryption. Modern cryptography concerns itself with the following objectives:

1. Confidentiality: The information is not understood by anyone for whom it was unintended. The prevention of Unaccredited with holding of information or resources.

2 Integrity: The information cannot be changed in storage or transmission between sender and intended receiver without The alteration being detected. The prevention of erroneous modification of information.

3. Availability: The prevention of unauthorized withholding of information or resources.

4. Authentication: The process of verifying that users are who they assert to be when logging onto a system.(the sender and receiver can confirm each others identity and the origin /destination of the information).

5. Authorization: The process of allowing only authorized user's access to sensitive information. Procedures and protocols that meet some or all of the above mentioned criteria are known as cryptosystems. Cryptosystems are often Thought to refer only to mathematical procedures and computer programs; however, they also incorporate the regulation of human behavior , such as choosing hard-to-guess passwords, logging off unnecessary systems, and not discussing diplomatic procedures with outsiders . In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer diplomatic information has proved a critical Factor in success in war and business. Privacy ensures that the only the transmitter and intended recipient of an Encrypted message can read the contents of the information that are transmitted from one place to another and Cannot be understood by any intermediate parties that may have intercepted the data stream . proposed work In the below fig1, 40 nodes were created and the nodes work in Normal Conditions. In AODV network , source node sends the Data packets to the destination node. Sending and receiving Data is done through route. The path is not fixed for the AODV protocol. According to demand network searches the shortest path to reach the destination.

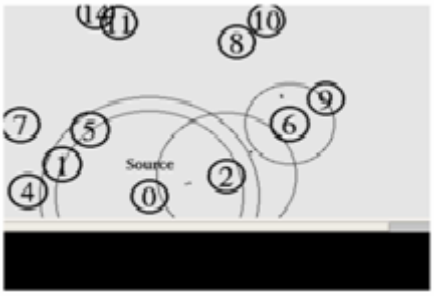

Fig. 1. Data transfer between created nodes

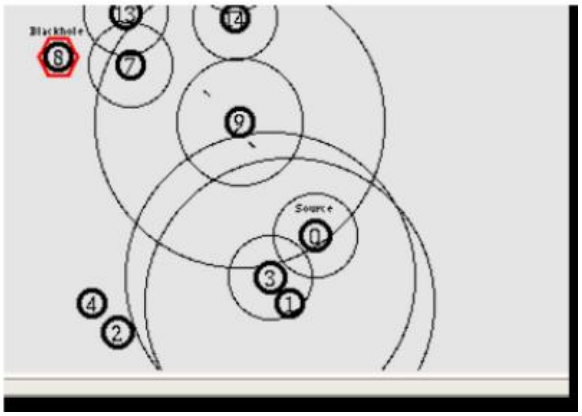

Fig. 2. Attacked by black hole node

The black hole node attacks the network, routing protocol is used By the attackers to show that it is having the shortest path to the node, for whose packets it want to intercepts In flooding based.

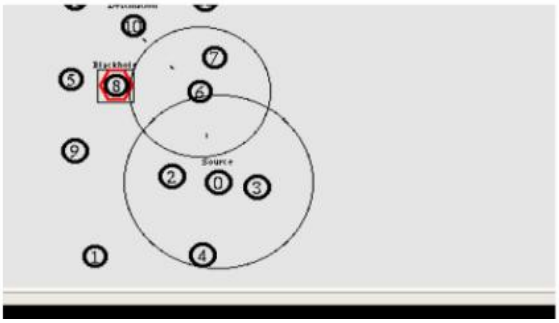

Fig. 3. After applying security mechanism

Protocol attacker listens the request for route, and after receiving route for destination node , attacker creates a reply having shortest route. A fake route is created, when the unknown reply reaches to the starting

node, before reply from the original node. In between the communicating nodes, if , malicious device has been inserted it will do anything to the packets passes through them. The first step in the man-in-the –middle attack, malicious device drops the packets in between them to perform the denial –of-service .

In security mechanism removal algorithm RC6 used to remove the attack. RC6 is a symmetric encryption algorithm and it is very fast and simple, suitable for hardware and software, and also it is adoptable to different word length processors ,with low memory requirements and provides high security .The RC6 algorithm asks for the Apply removal

Type- 1-if it is yes.
Type -0- if it is no.

Black hole node-here the maximum threshold condition is checked, if threshold value is less than the max sequence threshold value, then it is said to be black hole node. If threshold value is greater than the max sequence value then it is not a black hole node [3][7]. The removal function updates the Turn keep registration, increments the sequence number and checks all the sequence, if any node shows it a black hole node then it removes it. In remove request, black hole node is found when flag is 0, then encrypt. No black hole node is found when flag is 1, then decrypt.

II. Results And Conclusions

Table 1 Packet Delivary Ratio

	NORMAL AODV	ATTACK ON AODV	AFTER REMOVAL OF ATTACK
PDR	99.5	23.38	63.194

Table 2 Average End To End Delay

NORMAL	AODV	ATTACK ON AODV	AFTER REMOVAL OF ATTACK
DELAY	20.93 ms	0 ms	14.6062 ms

We conclude that from the above table for normal AODV the Packet delivery ratio is high because delay is high and it is not affected by any attack. PDR suddenly decreases and becomes Zero when AODV is attacked by the attacker. By applying the RC6 algorithm will remove the attack of pdr of AODV increases 40% gets increased here and delay also increases.

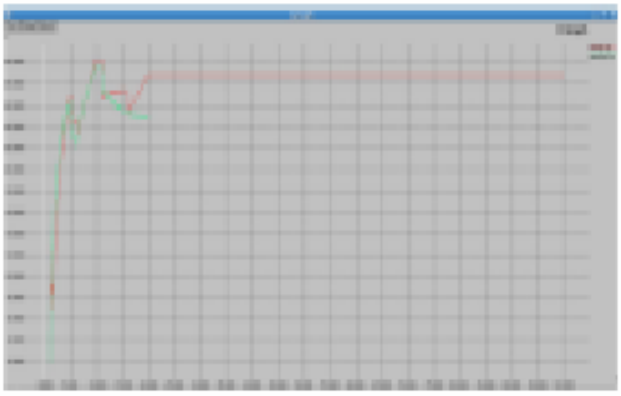

Fig 4: Energy

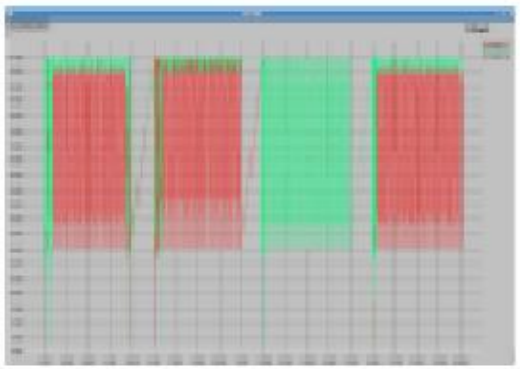

Fig 5: Throughput

III. Future Work

We will try to increase the PDR in future after applying the remove attack and try to increase the delay. The parameters like energy, throughput to be studied. Routing protocol will also be studied and checked the effect of raid on the other routing protocol.

Refferences

[1]. Asad Amir Pirzada , Chris Mc Donald and Amitava Datta, "Performance comparison of trust based reactive routing protocols" IEEE Transaction on mobile computing, vol.5,no. 6.june 2006.
[2]. Pramod kumar singh , Govindh sharma, "An Efficient prevention of black hole problem in AODV Routing Protocol in MANET, International Conference on Trust, Security and Privacy in computing and Communication.[4]
[3]. Morli pandya , Ashish shrivastava ,Rajiv Gandhi proudyogiki viswavidhyalaya" Improving the performance With security of AODV Routing protocol in MANETs "2013 Nirma University International conference on Engineering. [5]
[4]. Latha Tamil Selvan, V. Sankara narayanan, "Prevention of Co-operative Black hole attack in MANET", journal of Networks, volume .3,no .5 ,pp .13-20, May 2008.[2]
[5]. S. Deswal and S. Singh , "Implementation of Routing Security Aspect in AODV", Intl. Journal of computer theory And Engineering , Volume. 2 ,No. 1s Feb 2010.[3]
[6]. Seryvuth Tan, Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs" , 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing.
[7]. Sanjay k. Durandhar , Issac Woungang ,Raveena Mathurl, and Prasanth Kurana ,A Modified AODV against single and Collaborative Black hole attack in MANET's",2013 27th
[8]. International conference on Advanced Information NetworkingAnd Applications sssWorkshops.