Secure Active Detection Data Routing Protocol in Manets

[1]C.MUTHUPRIYA, [2]G.SIVAKUMAR, [3]Dr.K.RAMASAMY

[1] PG Student, [2] Assistant Professor, [3]Principal [1,2]P.S.R.Rengasamy College Of Engineering for women, Sivakasi

---

ABSTRACT

Border Gateway Protocol (BGP), which is used to distribute routing information between autonomous systems, is an important component of the Internet's routing infrastructure. Border
Gateway Protocol (BGP), is vulnerable to various attacks. It can cause prohibitively high global message overhead .BGP implements two attacks are Route flat damping and Minimum Route Advertisement Timer.RFD is designed to discourage to selection of unstable routers. MRAI limits the frequency of route announcement send to neighbour. In proposed method use secure active detection data routing protocol (ADDRP) used to establish unique path and key .ADDRP protocol is polynomial based protocol, computation is efficient. Active detection route to identify the black hole attack and mark the black location. It avoid the black hole attackers through the active creation number of detection routes. Detection route increase the lifetime and improve the data route security. we use in black hole attack are identify the filtering packets from attack source .single malicious node cause thousand of node become disconnected and other node eliminate such attacks.

Key Words - Secure Data Transmission, key Generation, ADDRP Protocol, Black Hole Attacks.

I.INTRODUCTION

MANET (Mobile Ad hoc network) is a set of mobile nodes consists of both a wireless transmitter and receivers connect with each other using bidirectional wireless links. Delegated as a peer to peer system each node or user in the network behaving as a data endpoint or intermediate repeater. MANETs are frequently self-forming, self- maintained and self-repairs itself process allowing for extreme network flexibility, which is generally used in penetrating mission applications like military purposes or emergency recovery, the minimum composition and quick distribution of nodes in preparation for work make MANET ready to be used in emergency circumstances. MANET is becoming more and more widely implemented in the industry. Manet is continuously self-maintained, support network of mobile devices that are connected without wires. These have highly dynamic and free topology. The contrary to traditional Network architecture, Manet does not require a stable network infrastructure; every single node works as both transmitter and the receiver. Nodes communicate directly with each other when they both with the communication range .The routing algorithm in MANET can be a single hop or multi hop .single hop communication is simpler in terms of structure and implementations but has lesser functions and application compared to multi hop communication. In multi hop communication, the destination is raised the transmission coverage of the source and hence the packets are forwarded via one or more intermediate node.

II. RELATED WORK

Yang Song, Lixin Gao, Arun Venkataramani the author explain Border Gateway Protocol (BGP), is vulnerable to various attacks. It can cause prohibitively high global message overhead .BGP implements two attacks are Route flat damping and Minimum Route Advertisement Timer. RFD is designed to discourage to selection of unstable routers. MRAI limits the frequency of route announcement send to neighbour. each router maintains a penalty associated with every route announced by neighbours. The penalty measures the instability of a route. Whenever a route is withdrawn, the route's penalty is increased by a fixed value. If the penalty of the route exceeds the *cut-off threshold*,the route cannot be used for selecting the best route, i.e., the route gets damped.

Xin Liu and Xiaowei Yang the author explain identify the several attack in bgp proposes a packet passport system to address this challenge. A packet passport efficiently and securely authenticates the source of a packet. A packet with a valid passport must have originated from the claimed source. The packet passport system can be incrementally deployed without introducing extra control messages. It also provides incentives for early adoption: a domain that deploys packet passport system can prevent other domains from spoofing its source identifiers.

Ke Zhang, Xiaoliang Zhao, S.Felix Wu the author explain selective dropping attack occurs when a malicious router intentionally drops incoming and

outgoing UPDATE messages, which results in data traffic being black holed or trapped in a loop. In this paper, we conduct a thorough analysis on this type of attack and advocate that new security countermeasures should be developed to detect and prevent such attack.

III.METHODOLOGY

1) Creating Network Formation
2) Data Transmission
3) ADDRP Protocol implementation
4) Key generation
5) Black hole attack implementation

CREATINGNETWORK FORMATION

In our simulations, the network area is 1200m*300m with 60 nodes initially and uniformly distributed .The channel capacity is 2mpbs.The Transmission range is 150m.A total UDP based CBR sessions are used to generate the network traffic. For each session, the data packet are generated with the size of 512 bytes in the rate of 16kpbs.The source –destination pairs are chose randomly from all nodes.

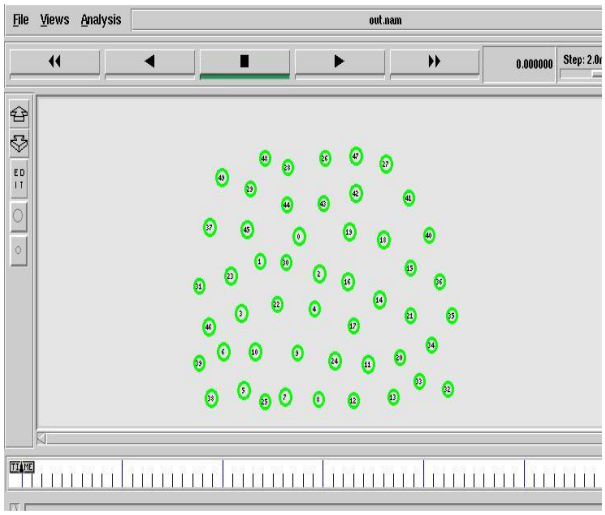

Fig 1 .1Creating Network Formation

SHORTEST PATH FINDING

On-demand reactive routing protocol that uses routing tables with one entry per destination. When a source node needs to find a route to a destination, it starts a route discovery process, based on flooding, to locate the destination node. Upon receiving a route request (RREQ) packet, intermediate nodes update their routing tables for a reverse route to the source. Shortest path routing to the process of finding path through a network that have minimum of distance, banndwidth, average traffic, speed. Initialize the array of smallest weight [u]=weights[vertex , u]. Here, we calculated the following: weight[u] =weights [vertex]=0 Mark v as next vertex for which smallest weight is found

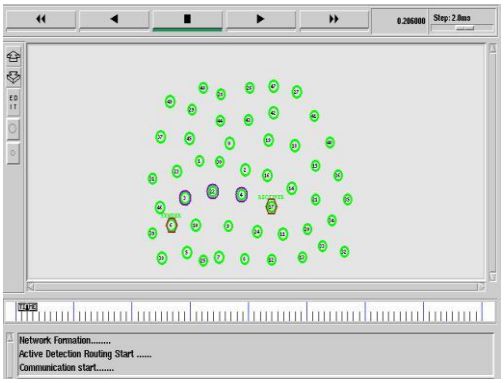

Fig 2. 1 Shortest Path Finding

DATA TRANSMISSION

Route request send to all intermediate nodes between source and destination. Route discovery for shortest and freshest path. When a source node needs to find a route to a destination, it starts a route discovery process, to locate the destination node. After reaches the destination node- Sends Route reply packets to source node. Transmit the data from source node to destination node through energy efficient intermediate nodes, If any path failure occurs again starts route discovery.

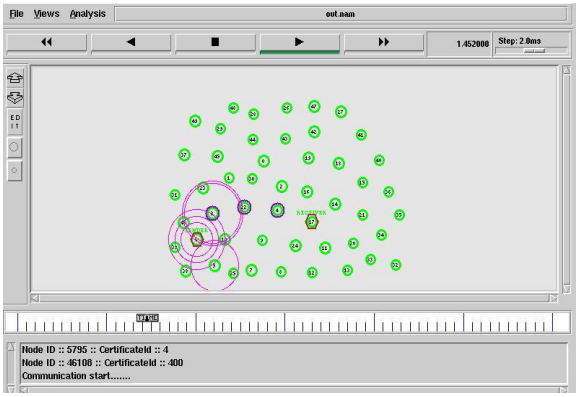

Fig 3.1 Data Transmission

PROTOCOL IMPLEMENTATION

The active detection data routing protocol are use to identify the attack behavior, and then mark the black hole location . Active detection routing,

nodal trust can be quickly obtained, and it can effectively guide the data route in choosing nodes with high trust to avoid black holes. Source node randomly selects an undetected neighbor node to create an active detection route The route will select a node with high trust for the next hop to avoid black holes, and thus improve the success ratio of reaching the destination.

KEY GENERATION

Each client in the network is assigned a key(private or public key) to send the data securely over the network. The cryptography algorithm named RSA is used here to generate key for the users. Two types of keys are one is public key another one is private key

PRIVATE KEY : The private key must kept secret. Detection of misbehavior nodes using Security Packet, then send communication between source to destination node.

PUBLIC KEY :The public key can be shared with everyone.

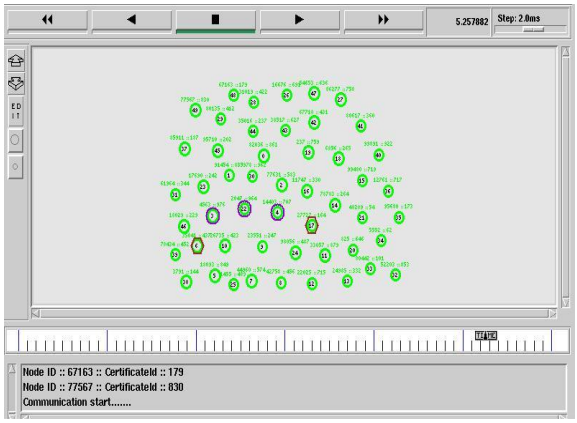

Fig 4.1 Key generation

MISBEHAVIOUR DETECTION

Route request send to all intermediate nodes between source S and destination D. Route discovery for shortest and freshest path using ADDRP. Check the Neighbor list. Detection of misbehavior nodes using Security Packet.Then send communication between source to destination node. we use Black hole attack can be classified in two way, one is Active black hole another passive attack. Active black hole attack: Node receives the RREQ packet and returns false RREP packet.

Active black node receives a data packet and discards it.

Types of Black hole attack, single BHA another one cooperated BHA.

Single BHA: In this type, there is only a single malicious node which is responsible for manipulating the routing tables entries of source node fitting itself into path between two communicating node.

Cooperated BHA: we use in cooperated BHA in our paper in cooperative attacks they are multiple attacks nodes which cooperate with each other to launch collaborative attack and increase the range it easy to spoof the replies attacks can bypass security mechanisms.

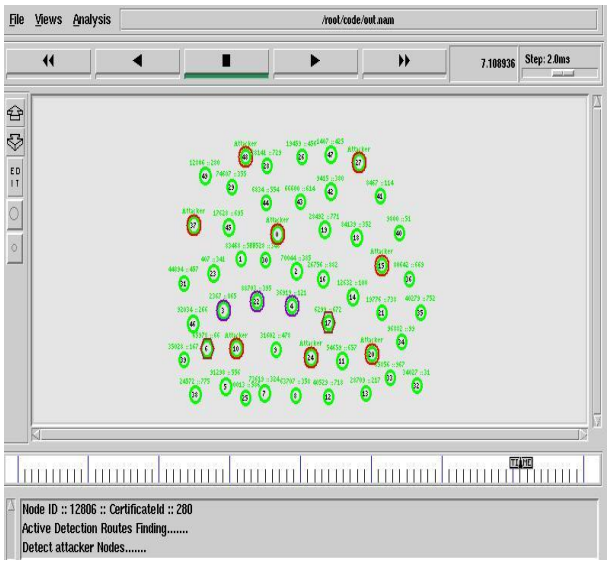

Fig 5.1Black hole attacker

IV PROPOSED METHOD

In this paper, we can propose private key Cryptography Technique that helps to reduce the network overhead. The count of acknowledged packet increases when the number of malicious node in network increases due to this reason, network overhead increases. Therefore, to reduce the network overhead we can use private key Cryptography Technique.
secure active detection data routing protocol (ADDRP) used to establish unique path and key
.ADDRP protocol is polynomial based protocol, computation is efficient .Active detection route to identify the black hole attack and mark the black location. It avoid the black hole attackers through the active creation number of detection routes. Detection route increase the lifetime and improve

the data route security. we use in black hole attack are identify the filtering packets from attack source
.single malicious node cause thousand of node become disconnected and other node eliminate such attacks.

System Architecture

The Proposed system uses the technique of RSA due to which private key Cryptography scheme provides three cryptography primitives called as Integrity, Confidentiality and Authentication. A key exchange mechanism eliminating the requirement of pre-distributed key, which examine the possibilities of adopting. For providing security encryption mechanism and RSA key exchange mechanism is to be considered. To perform encryption and decryption technique each node must have approach to other nodes neighborhood key. At origin, neighborhood key is encrypted with the public key of the receiver and transmitted to the terminal node. At terminal neighborhood key is decrypted with the node's own private key. The message specific key is having the advantage of making it to improve the security of the message
being forwarded in the wireless ad hoc network. .

RSA ALGORITHM

1. Rivert sharmits algorithm: It is asymmetric secure cipher cryptography. It is High performance and security.
2. RSA: It is public key cryptography can be used for encryption. The key management is an essential feature in RSA algorithm.

A.ENCRYPTION PROCESS:

Step1: An RSA algorithm key 'k' of 128-bit, 192, bit is chosen.
Step2: Encrypt message (M) using RSA algorithm above selected key K.
eM =RSA algorithm-encryption (M)
Step 3: RSA algorithm key K is encrypted by making use of RSA algorithm
Ek =RSA-encryption (k)

V . PERFORMANCE EVALUATION:

Simulation Configuration:

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with ubuntu. The system running with 3-GBRAM. In order to better compare our simulation. In NS2.34, the default configuration specifies 50 nodes in a flat space with size of 670×670m.The language we are using are TCL and AWK script. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 521B. In order to measure and compare the performance of our propone scheme, we adopt the following performance metrics:

PACKET DELIVERY RATIO

It defined by the ratio of number of the packets received by the destination node to the number of the packets sent by source node

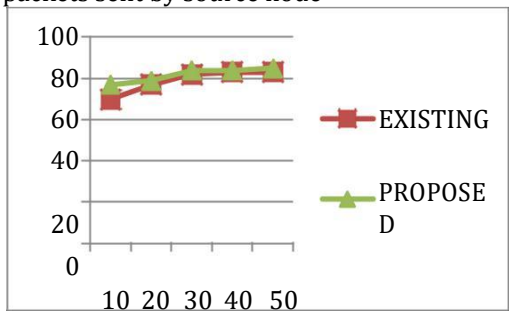

Fig 5.1 Packet Delivery Ratio

DELAY

The delay are received packets at destination is calculated sending time of the packet from the received time at the final destination.

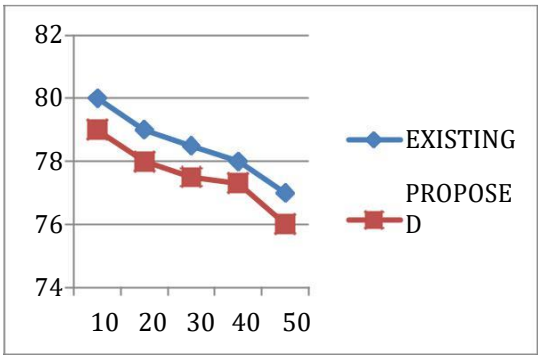

Fig 5.2 Delay

CONTROL OVERHEAD

Routing overhead refers ratio of routing related transmission.

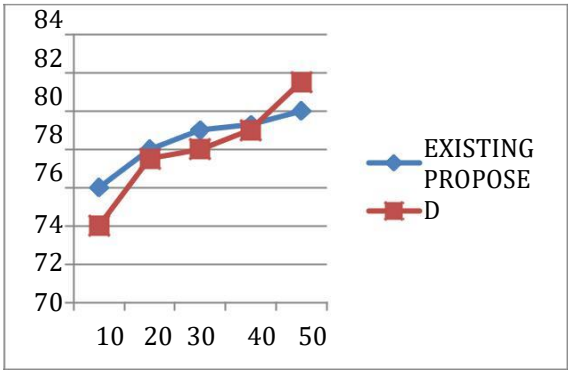

Fig 5.3 Control Overhead

V . CONCLUSION:

In these paper we have purpose the terminologies in security of MANET using method are concentrating only detection of malicious nodes

.we use private key cryptography used in encryption to strengthen the security of nodes. Detection of malicious node can be done by ADDRP using RSA algorithm. To improve security.

REFERENCE

1] Yang song, Senior Member,IEEE,Nan Kang, and Lixin Gao,"Identifying addressing and reachability and policy attack secure in BGP" IEEE
Transactions ,vol .no.3. 2016

2] Charles, karenseo " secure border gateway protocol real performance and issues", Volume 2 Issue 2, February 2014.

3] Dan Wendlandt, Rexford Princeton," Don't secure routing protocols, secure data delivery"IEEE Transaction,vol .no. 127 Newyork: 2013.

4] Biswas, Nandi "Host based IDS for NDP related attacks in spoofing in Proc.IEEE 25th Int.Conf.AINA, march 2013.

5] Yang Song, lixin gao , "Identifying and addressing protocol manipulation attacks in bgp,"
IEEE Trans. Ind. Electron., vol. 57,no. 3, pp. 840– 849, Mar. 2010.

6] Xin liu, xiaowei yang," Efficient and secure source authentication with packet passports,"IEEE Transaction, vol .no.56 Oct 2011.

7] Ke Zhang , felix wu," An analysis on selective Dropping attack in BGP,"in Wireless/Mobile Security.IEEE Transaction-2010

8] Doug Montgomery, oliver borchert, Richard Kuhn," Study bgp peering session attacks and impact on routing performance,"IEEE Trans. Mobile comput. vol .no. 6, May 2010

9] Yang, H., Ricciato, F., Lu, S., & Zhang, L.,
—Securing A Wireless World||, The Proceedings of
IEEE, Special Issue on Security and Cryptography, Vol. 24, No.2, (2006), pp. 443-454.