IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

SGR Protocol Implementation for Detection and Prevention of Black hole Attack in MANET

Nithya J[1], Shabana Sultana[2]

M. Tech, Dept. of Information Science, The National Institute of Engineering, Mysuru, India[1]

Associate Professor, Dept. of Computer Science, The National Institute of Engineering, Mysuru, India[2]

Abstract: In MANET communication plays a vital role in situations like natural calamities etc. It is more vulnerable to security issues since it does have fixed infrastructure. MANET is a collection of mobile nodes that forms a temporary network. One of the security issues is packet dropping. The dropping of packet may be caused due to link failure or malicious node present in the network. The most common attack in MANET is the black-hole attack. Ad-Hoc on demand distance vector (AODV) is prone to packet dropping attack. This paper presents a new protocol implementation named as Secure Geographic Routing (SGR) which deals with packet dropping in network layer. It also detects and prevents packet dropping.

Keywords: MANET, AODV, black hole attack, SGR.

I. INTRODUCTION

MANET is dynamic, self- configuring network that consists of nodes working in an ad-hoc manner without any fixed infrastructure. MANET is more prone to security attacks compared to wired medium. As the nodes in MANET are mobile they are free to move in all directions. The coverage area of the nodes changes as the nodes move away from the network. . Each node in MANET can act as both router and host, so it is autonomous. Even though MANET supports multiple hop communication between the nodes, the main security concern is that the packets should not be dropped by the malicious node or by misbehaved links.

In packet dropping attack, the malicious node will drop the packets and it will not allow the packet to forward to other nodes. If a node demands that it has a shortest path to destination then the protocol takes the demand as real and if there is any link break notified by a node then it will not be used for next transmission. AODV is more prone to Packet dropping attack.

A. AODV

AODV is a reactive protocol which is dynamic in nature. It uses a local broadcast message called “hello” message that provides connectivity information to the node. The source node will send a RREQ to its neighboring nodes. If the destination ID matches with the node ID of the receiving node, it will send a RREP to the source node else it forwards the RREQ to its neighboring nodes.

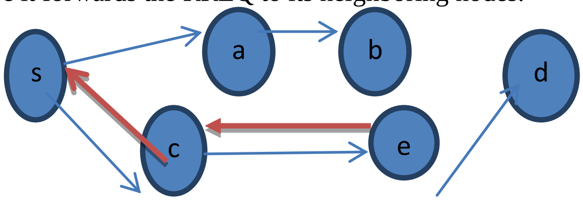

Fig 1: Working of AODV

RREQ
RREP

s → Source node, d → Destination node, a, b, c, e are intermediate nodes. The route selected to reach destination is s-c-e-d.

B. Black hole Attack

A malicious node present in the network may drop the packets willfully at the network layer in order to crash the network performance. This malicious node is termed as black-hole attack. It can collectively drop the packet.

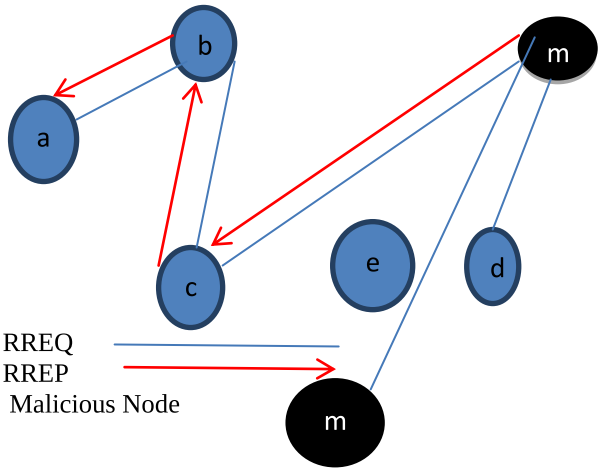

Fig 2: Black hole attack in AODV

In Fig 2, m is the malicious node. ’a’ and‘d’ are source and destination nodes .The source node ‘b’ broadcasts RREQ packet to its neighbors. After receiving this packet, each neighbor node is rebroadcasted if it has no route to the destination. The malicious node ‘m’ can claim that it has a shortest path to the destination and sends RREP to the source node ‘a’. The source node ‘a’ transmits the packet towards ‘m’. The node ‘m’ can drop all incoming packets or selected packets.

DOI 10.17148/IJARCCE.2016.54173

The node ‘m’ sends the data to the node ‘e’ instead of the destination node ‘d’.

In Secure Ad-hoc on Demand Distance Vector (SAODV), through secure path using RSA and CRC dropping of packet is detected and data is sent. More overhead occurs using RSA.

Most of the previous works proposed dropping of packets is due to malicious drops. In this paper, protocol SGR can handle these attacks that consider malicious node as the main cause for packet dropping. The proposed system can detect and prevent these attacks.

II. RELATED WORK

Many researchers have been interested to develop several mechanisms to identify the malicious nodes that present in the routing path, and then to take control over data packets and routing packets.

In order to establish a secured routing path, a scheme is proposed in AODV. On the completion of normal path discovery, the source node sends special control packets to obtain neighbor set of nodes that have sent RREP packet. If it gets more than one RREP, it compares with the neighbor set of nodes. If the difference is more than the previously defined threshold then it is considered as black-hole node. This paper reduces the black-hole attack but it cannot prevent from it.[7]

In paper[1] , SAODV is used to detect black hole attack. RSA is used for encryption and decryption of data. The drawback of RSA algorithm is that it creates more overhead.

In this paper, the author [8] proposes a method to overcome the black-hole attack i.e., to freeze all the intermediate node and make only the destination node to communicate with the RREP message. Authentication for RREP is not proposed; hence the attacker can spoof the IP address of the destination node and can act as destination node itself. This may cause black-hole attack.

The papers [9] and [12] proposes a credit based system. This system grants a credit score for cooperation among nodes. A credit is obtained by the node on forwarding packets to others. It uses the credit to send the packets to other nodes. In this method malicious node can get many credits by forwarding the packets that it receives from upstream nodes, hence selective dropping of packets cannot be detected.

The paper proposes a work done on reputation system [10]. The neighbor node gives the reputation of a node as bad when it has high packet dropping rate. This must be updated to all other nodes and it should be an important factor for selecting the routes. The disadvantage is that the malicious node pretends to have a good reputation by forwarding most of the packets to next hop, so that it leads to consider malicious node as trusted node.

A few authors specify the problem using cryptographic methods [3][4][5][6]. For example, the work in [11] uses bloom filters to make proof for forwarding to packets from each node. While the bloom-filters scheme is able to provide packet forwarding proof, the correctness of the proof is varying and there is a chance that it contains errors. In this case of detecting the selective packet dropping attack, accuracy of this scheme is very low. Hop to hop acknowledgements is based approach is proposed in [7]. Acknowledgements based method works only to count number of lost packets which does not give sufficient ground to detect the real actor that is causing packet loss.

The proposed protocol SGR considers dropping of both routing packet and data packets. It can detect and prevent the malicious node which causes the dropping of packets.

III. SECURE GEOGRAPHIC ROUTING

It’s a routing principle that relies on geographic position information. The basic idea of SGR is opportunistic routing. In addition, it adopts novel trust model to an effective metric against range of attacks from external to internal attacks in MANET. This protocol selects the minimum hop distance to reach the destination. SGR’s per-hop packet transmission is controlled and observed by sender instantly. Even though there is an attack in network this SGR protocol delivers the data to destination with integrity, confidentiality and non-repudiation.

This uses the location of the node in the network to selectively forward packets based on distance. Two techniques are used: Greedy forwarding and face routing. The forwarding is carried out on a greedy basis by selecting the node that is close to the destination. This process continues until the destination is reached. Whenever this method is not applicable or this method fails the algorithm uses face routing strategy to route around the communication voids and reaches the destination. Once the node comes in transmission range, the algorithm switches back to greedy forwarding, reducing the delay and increasing the performance.

In this approach after establishing the path from source to destination all the nodes in the path are agreed on coordinators public and private key. The source node encrypts the packet with the coordinator public key and sends to the neighboring node. The data is decrypted using private key. The source informs the coordinator that it has sent data to its closest node and it has received acknowledgement from that node. If the acknowledgement is not received it informs the coordinator node, it marks that node as black-hole node and chooses the different path to reach the destination.

A. Pseudo code:

```
Algorithm:Packet Forwarding
input : packet from srcnode, targetnode
Curr = srcnode
while curr != targetnode
    nextnode ← get geographical shortest node to target
    if next.node == true
    continue;
    end
    forward packet to nextnode
    forward packet to coordinator ( curr → nextnode)
     curr = nextnode;
end
```

```
wait for message from coordinator
if coordinator message
        node ← extract from coordinator node
        node.attacker  = true;
end
```

IV. PERFORMANCE EVALUATION AND SIMULATION RESULTS

For comparing performance of AODV, SAODV and SGR one simulator is used. It's based on java based tool. The focus is on truthful detection and prevention of packet dropping attack. The proper detection and prevention of this attack can be done by SGR.

As compared to AODV and SAODV, SGR has high detection rate. The result shows that SGR truthfully detects and prevents packet dropping attack in MANET.

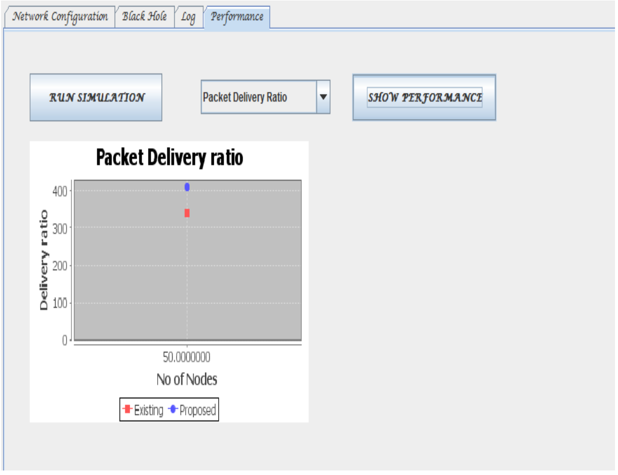

Fig 3: It shows the packet delivery ratio of Existing and proposed system.

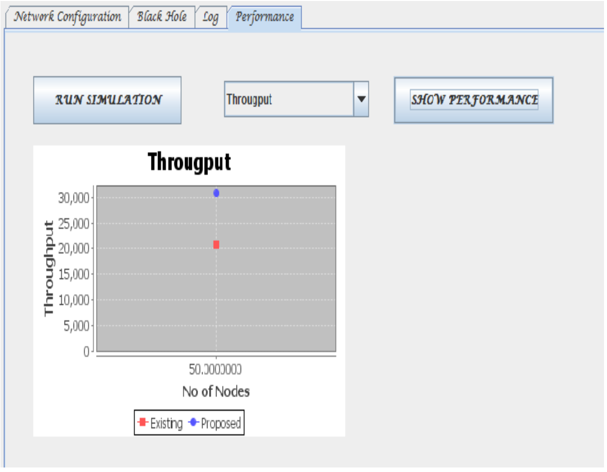

Fig 4: This shows the throughput of existing system and proposed system.

The simulation results are shown in graph .It depicts the packet dropping ratio and throughput.

In fig 3, the packet delivery ratio of proposed system and existing system is shown. Greater the packet delivery ratio better is the performance. The packet delivery ratio in proposed system is high compared to existing system.

The fig 4 depicts the throughput of the proposed system which is higher compared to existing system.

V. CONCLUSION

Mobile Ad-hoc Network (MANET) is a type of ad-hoc network which changes its location dynamically and configures itself. It do not have fixed infrastructure which is prone to different kinds of attacks. In this paper, it deals with detection and prevention of black-hole attacks. This paper proposes a new protocol named SGR, which is different from SAODV in security issues. The overhead in this paper is less. A coordinator node is introduced to control all the network operations and it is responsible for identifying packet dropping attack.

REFERENCES

[1] Nobel George , Sujitha M , vol 4,issue 7, July 2015,"Truthfull detection of packet dropping attack in MANET", DOI 10.17148/IJARCCE.2015.4773

[2] k. Balakrishnan, J Deng and P K Varshney, " TWO ACK: preventing selfishness in mobile ad-hoc networks " in Proc. IEEE Wireless Communication network conference 2005 pp.2137-2142.

[3] W. Mao , Modern cryptography: Theory and Practice, Pentice Hall publisher, July 2015.

[4] A. Shamir, How to share a secret, Communications of the ACM , 22(11):612-613, November 1979.

[5] L. Lamport, Password authentication with insecure communication, Communications of ACM, 24(11):770-772, November 1981.

[6] A J Menezes, P. C . Van Oorschotand S A Vanstone, Handbook of applied cryptogtaphy, CRC Press, October 1996.

[7] H Deng , W. Li and D P Agarwal, Routing security in wireless ad-hoc networks, IEEE commu. Mag.,40(10): 1775 October 2002.

[8] B. Sun Y.Gaun, J. Chen and U W pooch, Detecting blackhole attack in mobile ad-hoc network, In Proc. 5th Eurpoean Personal Mobile Commu.conference , Glasgow, UK, April 2003.

[9] L. Buttyan and J P Hubaux, Nuglets: A Virtual Currency to stimulate cooperation in self-organized mobile ad-hoc networks, Swiss Federal Institution of Technology, Lausanne, Switzerland, Tech. Rep. DSC/2001/001, January 2001.

[10] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup and A. Menezes, PGP in constrained wireless devices, In Proc. 9th USENIX security symposium, Denver, Colorado, August 2000.

[11] C Perkins, E. Belding-Royer and S Das, Ad-hoc On Demand Distance Vector (AODV) Routing, IETF RFC 3561(experimental), July 2003.

[12] S. Zhong, J. Chen and Y R Yang, "Sprite: A simple cheat- proof, credit based system for mobile ad-hoc networks", In Proc. IEEE INFO COM Conference, 2003, pp.1987-1997.

DOI 10.17148/IJARCCE.2016.54173