Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Identity Mapping Scheme with CBDS Approach to Secure MANET

By Gaurav Jain, Rajdeep Shaktawat & Kalpana Jain
College of Technology and Engineering, India

Abstract- A MANET is considered as self administrating network in which nodes are free to come and join to communicate with various nodes. A network which has a lot of advantages for its characteristics also has disadvantage of being attacked by some malicious node. Since MANET requires that each node should posses a unique, distinct identity, Sybil attack is one of the major threat to MANET. A Sybil attack is in which a node can have different physical identity to weak the distributed MANET system. In this paper, we propose a identity mapping scheme which is implemented with the collaborative bait detection scheme for securing MANET against Sybil attack, black hole attack and gray hole attack. Approach is merged with the CBDS approach for making system more secure against various attacks. Proposed scheme is simulated on NS2 and compared with the Sybil detection scheme on various performance metrics.

Keywords: *manet, secure network, identity mapping scheme, sybil attack, black hole attack, gray hole attack.*

GJCST-E Classification : *D.2.1*

Identity Mapping Scheme with CBDS Approach to Secure MANET

Gaurav Jain [α], Rajdeep Shaktawat [σ] & Kalpana Jain [ρ]

Abstract- A MANET is considered as self administrating network in which nodes are free to come and join to communicate with various nodes. A network which has a lot of advantages for its characteristics also has disadvantage of being attacked by some malicious node. Since MANET requires that each node should posses a unique, distinct identity, Sybil attack is one of the major threat to MANET. A Sybil attack is in which a node can have different physical identity to weak the distributed MANET system. In this paper, we propose a identity mapping scheme which is implemented with the collaborative bait detection scheme for securing MANET against Sybil attack, black hole attack and gray hole attack. Approach is merged with the CBDS approach for making system more secure against various attacks. Proposed scheme is simulated on NS2 and compared with the Sybil detection scheme on various performance metrics.

Keywords: manet, secure network, identity mapping scheme, sybil attack, black hole attack, gray hole attack.

I. Introduction

The MANET (Mobile Ad hoc Network) are widely used in various applications like military application and in emergency operations due to mobility of nodes in wireless network. Every node depends on one another so coordination between them become important, if any of the node misbehave or do not coordinate, it can lead to destruction of whole MANET. One such attack is Sybil Attack in which a node can posses multiple identity .In such type of attack a node posses some other node identity and thus participate itself on behalf of genuine node, thus harming the integrity and security among nodes.

A network in which any node can join and leaves the network without any central authentication, breaching such a network is simple for any malicious node. So the security comes out to be the important aspect in MANET. In MANET each node should have only a single identity through which it can communicate with other nodes in the network. In MANET each node act as a host as well as router, this significant feature of MANET also comes with the serious drawback of security issue. As path between the source and destination has number of nodes in between which act as router and transfer data from one end to another. The nodes are free to move so there is no fix topology in this network, this gives a fair chance to any malicious node to come and break the integrity of the network.

In this approach, there is collaborative bait detection scheme which is merged with the ID mapping scheme to secure the MANET against various black hole attack, gray hole attack and Sybil attack.

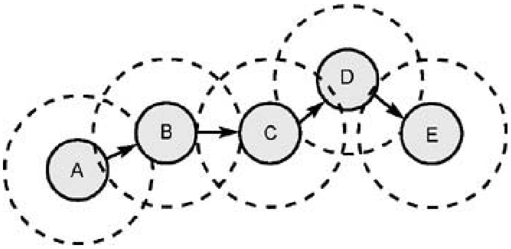


Fig.1: A Simple MANET structure

A node can transfer or communicate with the node which falls in their radio range. Before the data transmission takes place between the source and destination, source needs to find out the location of the destination as in MANET nodes are free to join or leave the network or move freely. There is no central authority which governs the whole network or the communication so it totally depends upon the nodes to find the destination node and its path. Intermediate nodes work during the path formation as well as during the data transmission. Broadly there are two categories of routing protocols in MANET, one in which path formation or routing takes place when source needs to communicate with the destination and second in which all nodes exchange some packets continuously to keep the path for each node. As there is power constraint in MANET on demand routing protocols are much preferred than table driven protocols.

MANET network is much exposed to various threats due to its characteristics. There are various attacks for which MANET is exposed, held at different layers. Many attacks are performed during routing like a malicious node can change various fields of route discovery packet which can result in a path formation in which malicious node fall, after that a malicious node can perform various attacks like black hole and gray hole attack which result in rapid degradation of network as malicious node starts dropping of data packet for all connection in black hole attack and for a particular connection in gray hole attack. The other major attack is Sybil attack in which attacker can disrupt location-based or multipath routing by participating in the routing.

Author α σ ρ: Computer Science and Engineering, College of Technology and Engineering, India. e-mails: shaktawat.rd@gmail.com, gauravpamecha20@gmail.com, kalpana_jain2@rediffmail.com

a) Characteristics of MANET

Dynamic Topology : In MANET the nodes are free to move with different speed , due to which the topology changes frequently.

Security: MANET is an open network no authentication of nodes. So they are more prone to attacks like black hole, grayhole , Sybil and other attacks.
Multi hop routing: When a node tries to send information to other nodes which is out of its scope, the packet forwarded via one or more intermediate nodes.

Distributed operation: There is no central control or authority in MANET which controls the movement of nodes in MANET. The nodes collaborate and broadcast among themselves.

b) Challenges in MANET and Security

Limited bandwith : The narrow radio band results in decreased data rates compared to the wireless networks. Hence minimum use of bandwidth is necessary by keeping low overhead as possible.

Routing Overhead: In MANET, nodes often change their location within network, which leads to unnecessary routing overhead.

Packet Loss : There is higher packet loss because of increased collisions by the presence of hidden terminals, presence of interference, unidirectional links, frequent path breaks due to mobility of nodes.
Hidden terminal problem: The hidden terminal problem refers to the strike of packets at a accepting node due to the simultaneous transmission of those nodes that are not within the direct communication range of the sender, although are in the transmission range of the receiver

Security threats: As the MANET is liable to eavesdropping and wireless system functionality is established through node cooperation, mobile ad hoc networks are exposed to numerous security attack like blackhole, grayhole ,Sybil attacks etc.

II. Background details

There are two approach for security in all network one is Preventive approach that is cryptographic approach in which different cryptography processes are used for guard and second is reactive approach in which systems like intrusion detection systems are used for tracking down attacks like IP spoofing, blackhole, grayhole, Sybil attack etc. This paper will concentrate in one protocol DSR standardized by IETF. The fundamental difference that is in between DSR networks and established internet protocol is the security. That draws attention of many researchers over this note. DSR networks are more prone to any attacks. Attacks in DSR network is not only constitute of modification, eavesdropping, Sybil attacks etc. but also like nodes not cooperating in routing, intentionally dropping the packets, changing contents that attract source and destination to choose This paper will discuss approaches that are used so far for security and the proposed scheme proves out to be more capable in terms of security with minimum overhead and maximum security. This paper proposed a detection scheme called the cooperative bait detection scheme (CBDS) with ID mapping scheme, which aims at identifying and hampering malicious nodes launching grayhole, blackhole along with Sybil attack in MANET.

a) Coolabrative Bait Detection Scheme (CBDS) Approach

The cooperative bait detection scheme (CBDS), which plan at detecting and preventing malicious nodes launching grayhole/collaborative blackhole attacks in MANETs. In this approach, the source node stochastically selects an adjacent node with which to collaborate, such that the address of this node is used as bait destination address to bait malicious nodes to send a route reply RREP information. Malicious nodes are then detected and prevented from participating in the routing procedure, applying a reverse tracing technique. In this scheme, it is assumed that when a significant drop occurs in the packet transmission ratio, an alarm is emit by the destination node back to the source node to trigger the detection mechanism again.
CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive feedback at the successive steps in order to lower the resource wastage. CBDS is DSR-based. As such, it can identify all the addresses of nodes in the elected routing way from a source to destination after the source has accepted the RREP message. However, the source node can not necessary capable to identify which of the intermediate nodes has the routing knowledge to the destination or who has the reply RREP message or the malicious node reply forged RREP.

This scenario can result in including the source node sending its packets through the fake shortest path chosen by the malicious knot, can result to a blackhole attack. To resolve this issue, the function of HELLO message isjoined to the CBDS to assist each node in identifying which nodes are their adjacent nodes within one hop. This function helps in sending the bait address to seduce the malicious nodes and to utilize the reverse tracing program of the CBDS to identify the perfect location of malicious nodes. The baiting RREQ packets are similar to the original RREQ packets, but their target address is the bait address.

i. Initial Bait Setup

The aim of the bait phase is to seduce a malicious node to send a reply RREP by sending the bait RREQ which it has used to announce itself of containing the shortest path to the node that detains the packets that were converted. To accomplish this goal, the subsequent method is created to generate the destination address of the bait RREQ'. The source node randomly pick an adjacent node, i.e., *nr*, within its one-hop neighborhood nodes and cooperates with this node by catching its address as the destination location of the bait RREQ'. Since each baiting is done stochastically and the adjacent node could be altered if the node moved, the bait would not remain same. The bait phase is activated whenever the bait RREQ' is sent earlier to seek the first routing path.

ii. *Reverse Tracing Setup*

The reverse tracing approach is used to discover the nature of mischievous nodes through the route reply to the RREQ' message. If a mischievous node has taken the RREQ, it will reply with a fake RREP. Accordingly, the reverse tracing action will be applied for nodes receiving the RREP, with the aim to find out the malicious path information and the momentary trusted region in the route. It should be emphasized that the CBDS is capable of detecting more than one malicious node parallel meanwhile these nodes send reply RREPs. Indeed, when a malicious node, for example, *nm*, answer with a fake RREP, an address table P = {n1, . nk, . . . nm, . . . nr} is stored in the RREP. If node *nk* receive the RREP, it will isolate the *P* list through the destination address *n*1 of the RREP in the IP field and get the address list Kk = {n1, . . . nk}, where *Kk* show the route knowledge from root node *n*1 to destination node *nk*. Then, node *nk* will identify the diversity between the address list P = {n1, . nk, . . . nm, . . . nr} stored in the RREP and Kk = {n1, . . . nk}

b) *RSS Sybil detection Approach*

In particular, this scheme utilizes the Received Signal Strength (RSS) value in order to identify among the legitimate and Sybil knot. It presume that the attacker conjoin the network with its one identity, and that malicious nodes do not conspire with one another. It also infer that nodes do not rise or drop their transmit power.

The difference between a new legal node and a new Sybil identity can be made found on their neighbourhood joining nature.

The new authentic nodes become neighbours when they arrive inside the radio range of another nodes; thus their first RSS at the receiver node will be low .

On contradiction a Sybil attacker, which is already a neighbour, will result its new identity to appear suddenly in the neighbourhood.

Each node keep a list of neighbours in the form

<Address, Rss-List <time, rss>>.

Every node will catch and stock the signal strength of the transmissions received from its neighbouring nodes.

It Does not detect Sybil node present in root

III. The Proposed Method

a) *ID Mapping Scheme for Sybil Attack*

In the CBDS approach, the reverse tracing technique is used to find the blackhole and grayhole attack in MANET. The address list has been attached with the RREP, by splitting out and finds the intersection of that address list only we find out temporary trusted identities and the malicious list. So, identity of a node is very much important in the reverser tracing technique.

But in Sybil attack, more than one identity can correspond to a single entity. To detect the Sybil identity present in the network, we are going to mapping the id with the entity or node in the network. For that, we propose a new scheme called **as ID mapping scheme.**

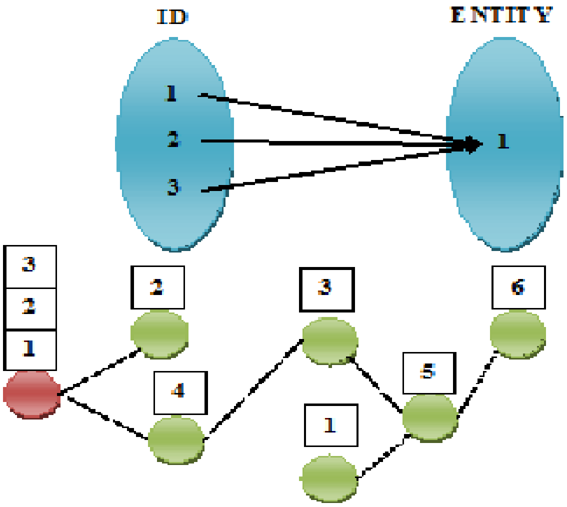
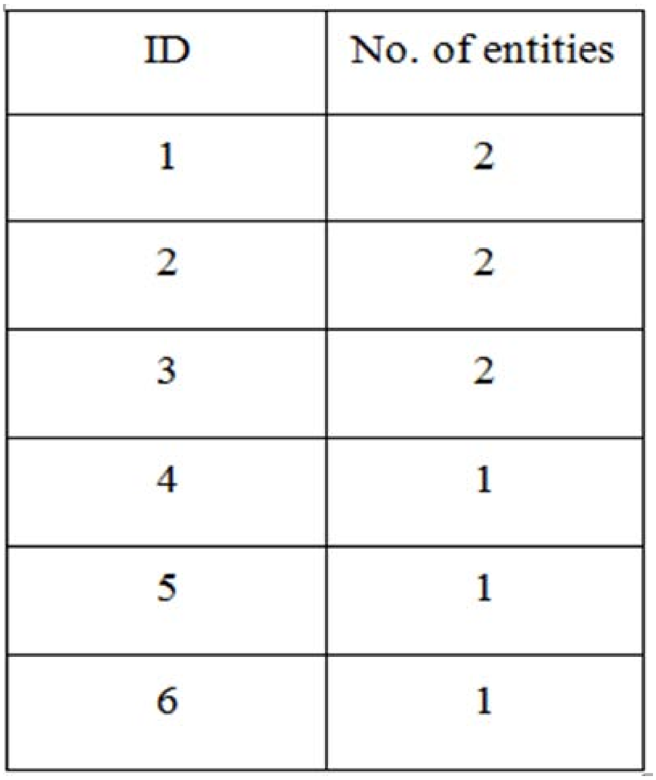


Fig 2 : Id Mapping

After detecting the temporary trusted list the source node the source node check for Sybil identity in the network. The Sybil node is having more than one identity to act as multiple nodes in the network simultaneously. The source node runs the following algorithm to detect the Sybil identities in the network. Before that, the source node maintains a table in the following format

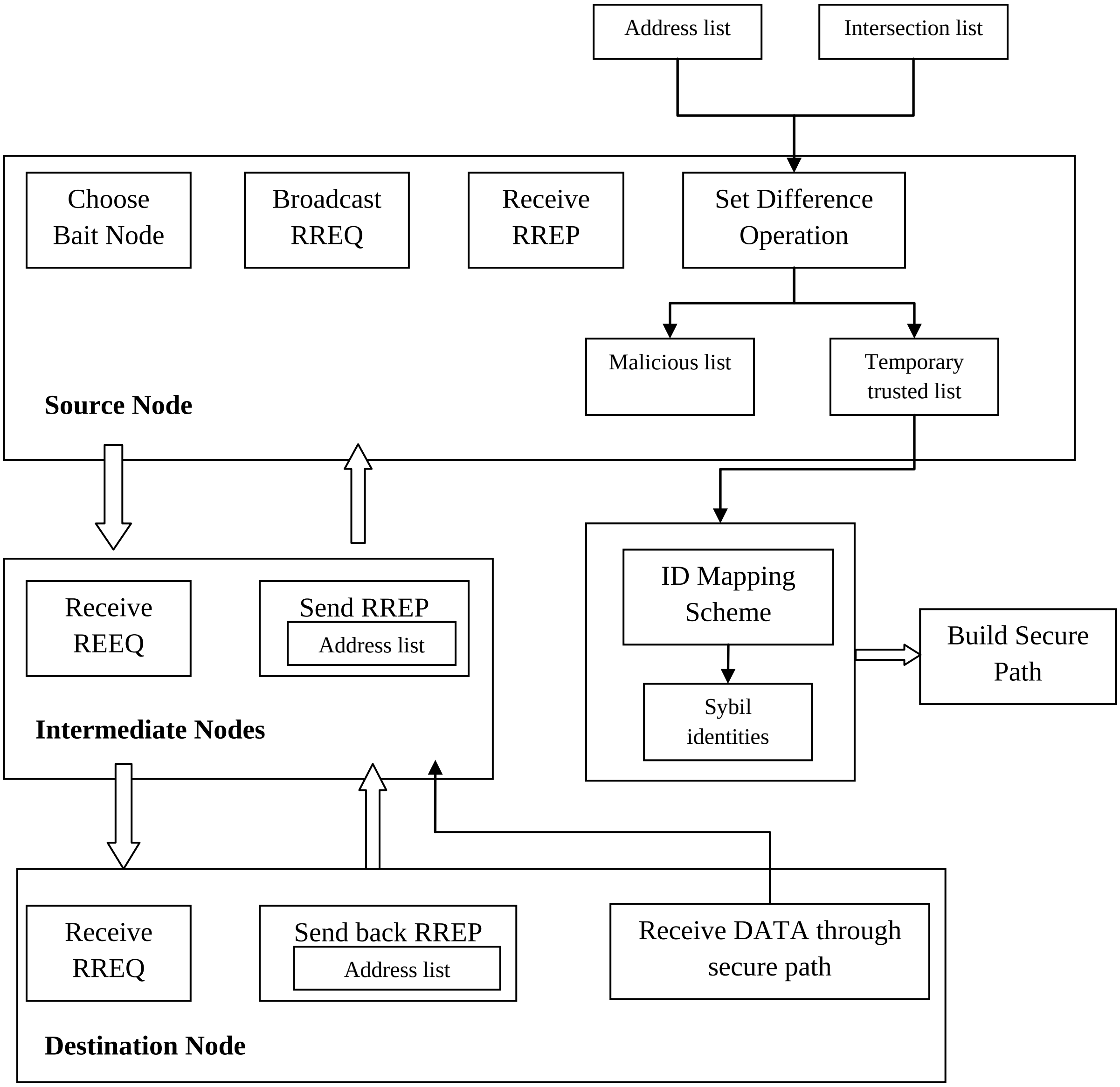


ID	No. of entities
1	2
2	2
3	2
4	1
5	1
6	1

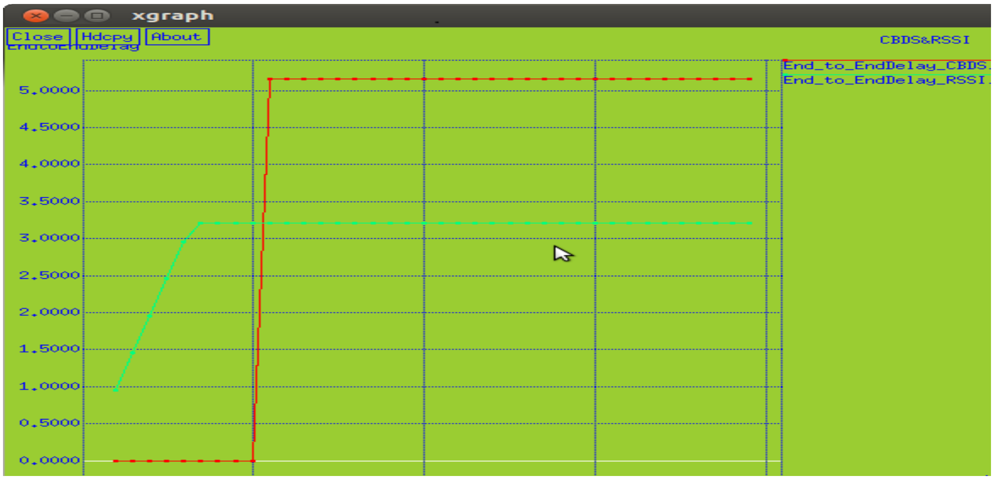
ID mapping scheme:

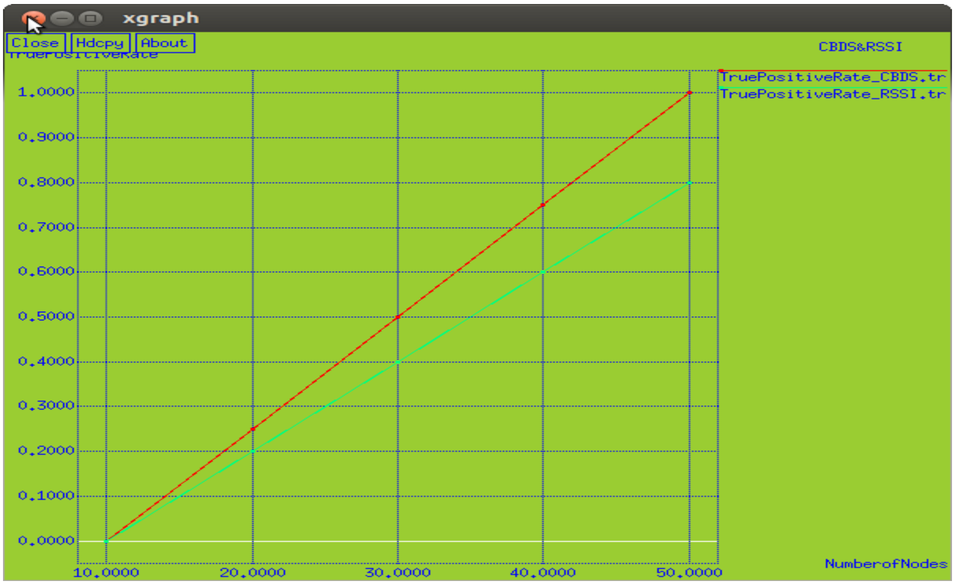
```
For each node 'n' in trusted list
{
    Nid=n
    While (Not reach all the nodes) {
        Source node broad cast hello message
        If (source receives reply with source address n) {
            Increment no. of entities by 1
        }
    }
    If(no. of entities>1) {
        Insert node with id 'n' to the malicious list
    }
}
```

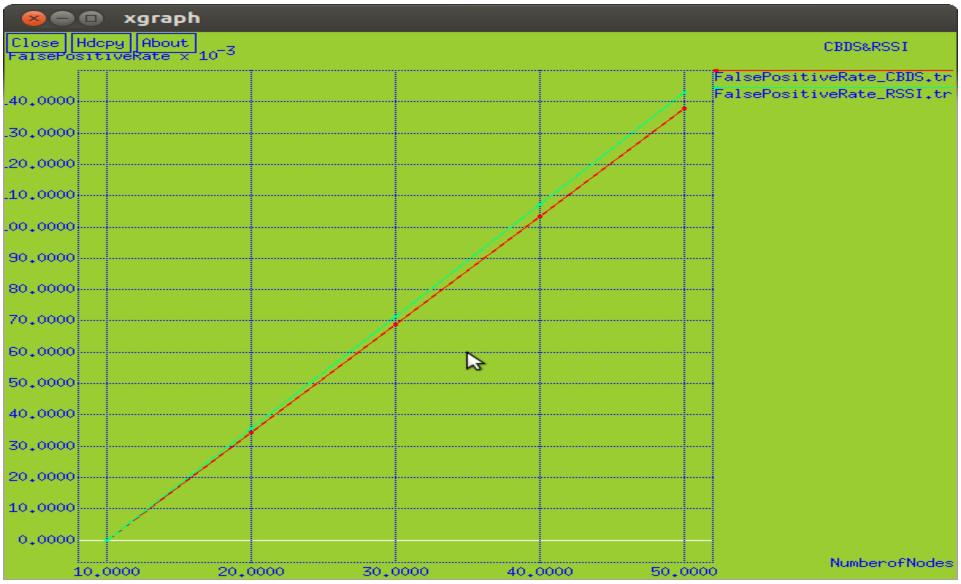
Block Diagram

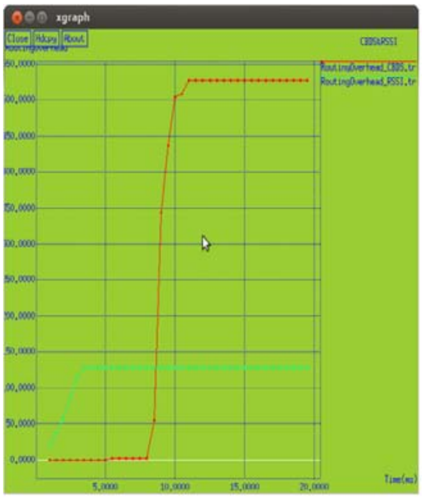


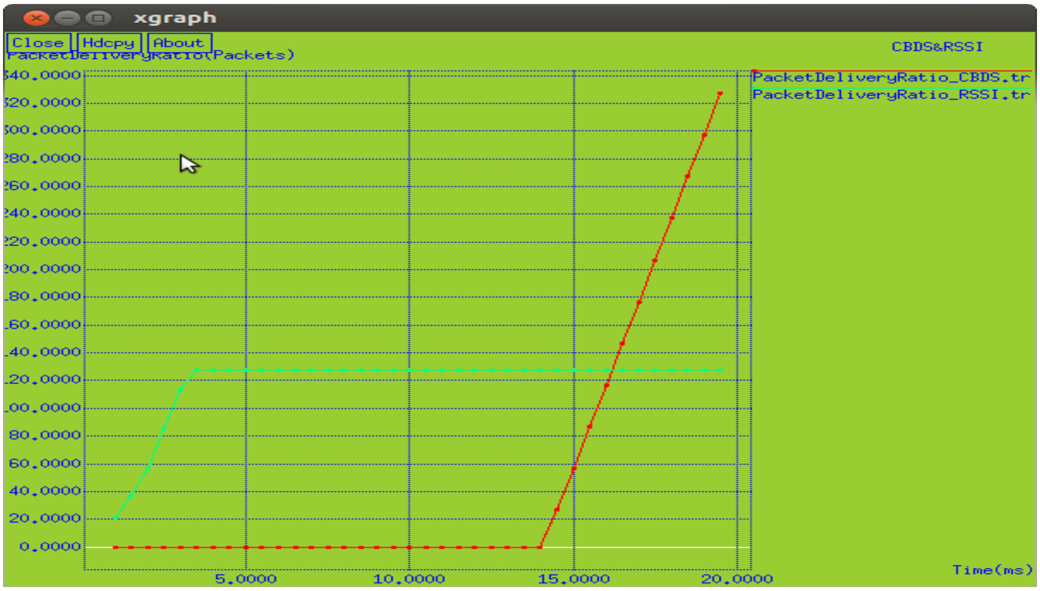
IV. Implementation and Results




xgraph
Close
Hdcpy
About
CBDS&RSSI
TruePositiveRate
1.0000
0.9000
0.8000
0.7000
0.6000
0.5000
0.4000
0.3000
0.2000
0.1000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
TruePositiveRate_CBDS.tr
TruePositiveRate_RSSI.tr
NumberofNodes


xgraph
Close
Hdcpy
About
CBDS&RSSI
FalsePositiveRate x 10-3
40.0000
30.0000
20.0000
10.0000
00.0000
90.0000
80.0000
70.0000
60.0000
50.0000
40.0000
30.0000
20.0000
10.0000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
FalsePositiveRate_CBDS.tr
FalsePositiveRate_RSSI.tr
NumberofNodes


xgraph
Close
Hdcpy
About
CBDS&RSSI
RoutingOverhead
50.0000
00.0000
50.0000
00.0000
50.0000
00.0000
50.0000
00.0000
50.0000
00.0000
50.0000
0.0000
5.0000
10.0000
15.0000
20.0000
RoutingOverhead_CBDS.tr
RoutingOverhead_RSSI.tr
Time(ms)



V. Conclusion and Future Work

This paper attempts to resolve the problem of presence of malicious node which leads to black hole/ gray hole and Sybil attack in MANET which is referred to as the cooperative bait detection scheme (CBDS) with ID Mapping Scheme, that integrates the advantages of both proactive and reactive defense architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. In this project, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANET's under gray/collaborative blackhole attacks. The ID Mapping scheme is used to detect the Sybil node present in the network. Our simulation results revealed that the CBDS with ID mapping scheme outperforms than the existing method RSSI based Sybil detection scheme in terms of routing overhead, End to End delay and packet delivery ratio.

References Références Referencias

1. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.
2. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. MobileComput.*, vol. 6, no. 5, pp. 536–550, May 2007.
3. S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE Trans., vol. 7, no. 2, June 2013.
4. W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in *Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst.*, New Delhi, India, Sep. 2009.
5. I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 13–64, 2003.
6. J. R. Douceur, "The Sybil attack," presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.
7. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defences," presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268.
8. B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. 4th Workshop HotNets*, 2005, pp. 1–6.
9. K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes," in *Security in Distributed and Networking Systems* (Computer and Network Security). Singapore: World Scientific, 2007.
10. S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks," in *Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol.*, 2010, pp. 17–24.

This page is intentionally left blank