Dynamic Network Topology to Exclude Malicious Attacks

[1]Dr. Rajani R,
Dept. of MCA,
Narayana Engineering College,
(JNTUA)
Nellore, A.P, INDIA
rajaninec@gmail.com

[2]Asia SK,
Dept. of MCA,
Narayana Engineering College,
(JNTUA)
Nellore, A.P, INDIA
rajaninec@gmail.com

[3]Bhagya Lakshmi G
Dept. of MCA,
Narayana Engineering College,
(JNTUA)
Nellore, A.P, INDIA
rajaninec@gmail.com

ABSTRACT: **Mobile ad hoc networks (MANETs) are exposed to many adversarial networking attacks due to the presence of dynamic infrastructure, and its nature of open transmission media. These characteristics make the design of routing protocols in MANETs a challenging task. In this paper, we propose an evolutionary scheme called self-cooperative trusting nodes (SCTN) that mimic the cognitive process of human beings and relies on trust-level information to prevent various routing disruption attacks. In this scheme, trust information is exchanged between mobile nodes and the nodes will start to analyse received trust information based on their own intelligence. Eventually, each node tries to exclude malicious attacks dynamically.**

Keywords: Self-cooperative, Cognitive process, Trust Level Information, Disruption Attacks, Malicious Attacks

I. INTRODUCTION

The abnormal growth of mobile ad hoc networks (MANETs) can be seen now-a-days due to the rapid development and usage of mobile devices in the society. MANETs consist of a group of wireless mobile nodes and they exchange data among themselves dynamically without relying on any centralized administration or fixed base station. MANETs can be easily established in a variety of disparate situations, such as rescue, emergency operations, and battlefield communications due to their Self-cooperative nature. However, this mobility and Self-cooperative nature of MANETs may cause the change in network topology in an unpredictable way. Each mobile node with limited transmission range seek assistance from its neighbouring nodes for data transmissions. Therefore, as a result, the MANETs largely depends on the reliable routing among nodes to prove their performance.

Extensive studies have been conducted on many routing protocols in MANETs, yet they are vulnerable to routing disruption attackers. We can see Black hole and Gray-hole attacks in MANETs. Considerable amount of data packets can be dropped silently in black hole attack. In gray-hole attacks, instead of dropping the attackers may selectively forward those data packets.

It is common in MANETs that some malicious nodes may hide in the network and drop the packets in order to save the energy or break the network operation due to the open nature of MANETs.

To overcome the above said challenges faced by MANETs, in this paper we propose an evolutionary scheme called self-cooperative trusting nodes (SCTN) that mimic the cognitive process of human beings and relies on trust-level information to prevent various routing disruption attacks. In this scheme, trust information is exchanged between mobile nodes and the nodes will start to analyse received trust information based on their intelligence. In this scheme, every node tries to evaluate the trust level of neighbouring nodes independently and they share the same information with their direct neighbours to help the other nodes. This self-detection process will influence the nature of a node i.e., optimistic or pessimistic towards the network.

II. RELATED WORK

Network performance always relies on secure routing. Conventional secure routing protocols employ a variety of cryptographic tools to prevent active attackers from injecting false information into a network. A careful review of these secure routing protocols reveals that most of them presume the existence of a centralized or distributed third party in the network. This assumption is also coupled with pre-existing shared secret keys between nodes inside the network. However, these assumptions are invalid in MANETs. As we know, MANETs have the diverse nature of being improper, thus they inherently oppose the dependence upon prerequisites. Furthermore, cryptographic operations, such as computing digital signature and verification, are considered computationally expensive on resource con-strained mobile nodes. The most important issue in these secure routing protocols is that they cannot identify those passive attacks, such as passive black hole attacks and gray-hole attacks. Consequently, trust based routing schemes become a new approach to ensure reliable routing in MANETs.

Disadvantages of Existing System

- The faster malicious nodes move, the larger region they can cover.
- Due to the open nature of MANETs, it is rather common that some malicious nodes may hide in the network and drop the packets in order to save the energy or break the network operation.

III. PROPOSED SYSTEM

In this paper, we demonstrate that mobility can actually be helpful to enhance security. We develop a generic trust evaluation system that can be easily applied on top of existing routing protocols. This SCTN scheme is capable of preventing not only conventional routing disruption attack attacker s, but also those internal attackers who even know how the security mechanism works. This SCTN scheme requires direct neighbors to exchange trust information periodically. Each node puts more confidence in the trust information explored by self-detection than the one derived based on shared results from neighbors. Moreover, this trust information can only be modified when the node obtains new information with a higher or equal privilege level.

IV. WORK FLOW PROCESS

As specified, our scheme accomplishes the task by following the below mentioned algorithms or modules.

A. Sender Module

- In this module, sender can identify the trust information and share the same information with router.
- The sender can browse the file and send the file to receiver.

B. Receiver Module

- In this module, receiver can receive file and save file.

C. Router Module

- In this module, router is responsible for routing the data from sender to receiver.
- It can handle trust information of nodes, node status, file information, attacker details.
- Once it receives request to send data to receive from sender, it checks the node status and cooperative behavior of the nodes, then, find the routing path and transmit the file to receiver in the path.
- If any attacker attacks the file using various types of attacks, it can identify the attacker details and also the type of attack.

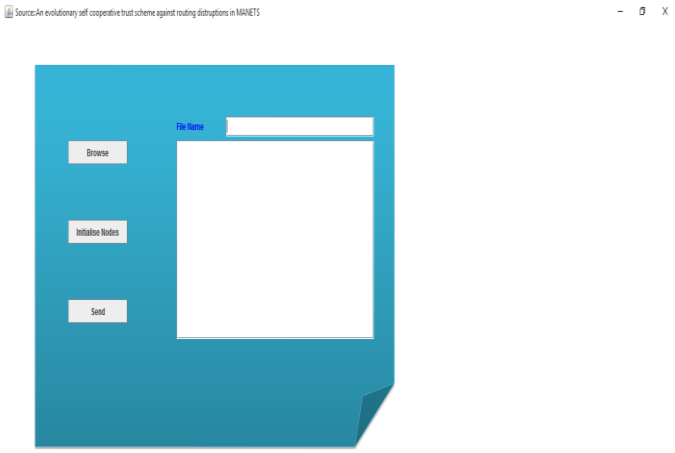
D. Attacker Module

- In this module, attacker attacks the file using different type of attacks.
- There are two types of routing disruption attacks that can be easily launched in MANETs: (1) Active black hole attack, (2) Gray-hole attack.

V. EXPERIMENTAL RESULT

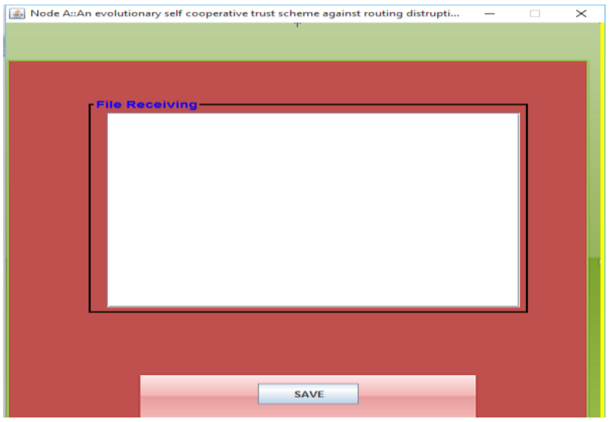
Source or Sender :

Using this Screen, the Sender can Browse for the required file and send the file to Receiver.


Source::An evolutionary self cooperative trust scheme against routing distruptions in MANETS
File Name
Browse
Initialise Nodes
Send

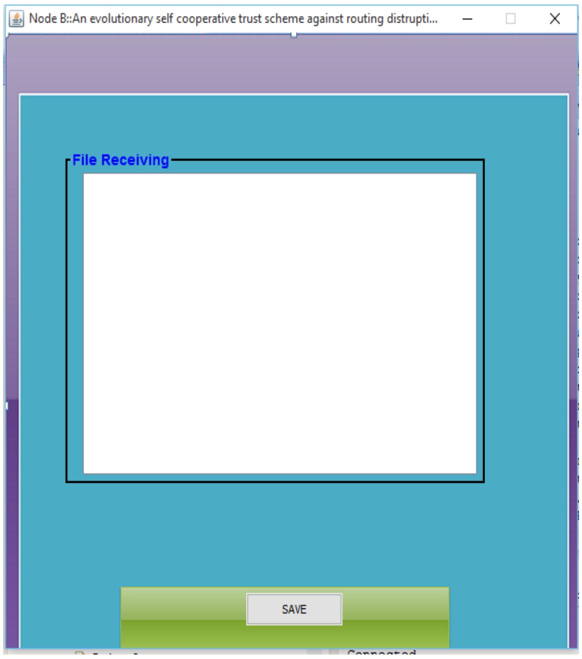
Node A :

This screen demonstrates one of the destination node, which receives the file from the source node.


Node A::An evolutionary self cooperative trust scheme against routing disrupti...
File Receiving
SAVE

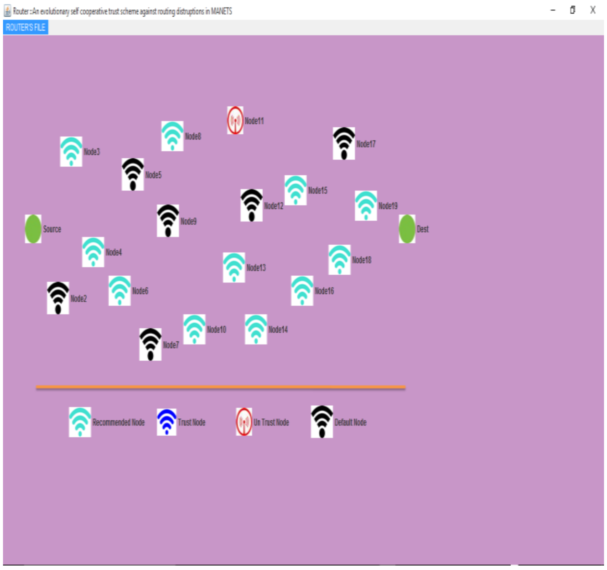
Node B :

It is also one of the destination Nodes, which receives the file from the source node.


Node B::An evolutionary self cooperative trust scheme against routing distrupti...
File Receiving
SAVE
Connected

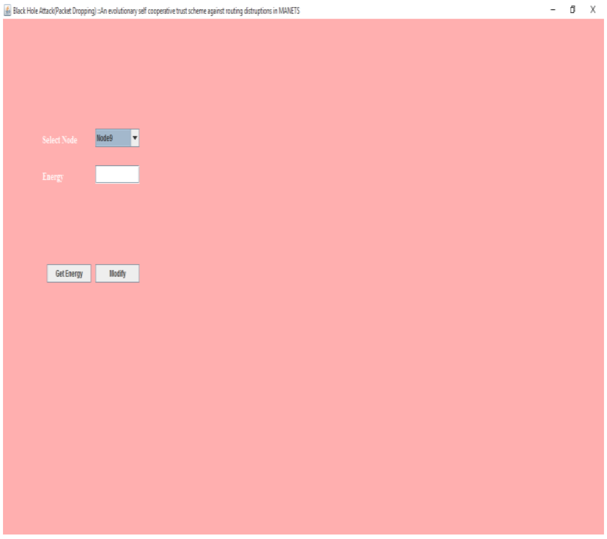
Router:

Router receives the request from the sender requesting for sending data to receiver. Here, the router checks the node status and cooperative behaviour of the nodes then find the routing path and transmit the file to receiver in that path.



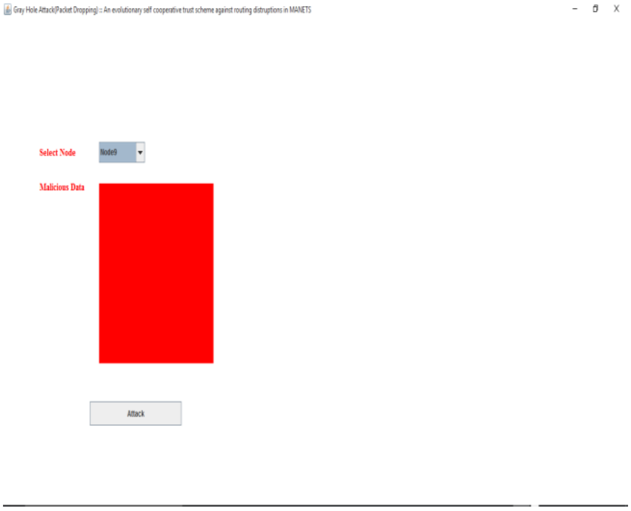
Black Hole Attack :

It is one of the routing disruption attacks, Attacker can Modify the Energy of the particular node.


Black Hole Attack(Packet Dropping) ::An evolutionary self cooperative trust scheme against routing distruptions in MANETS
Select Node
Node9
Energy
Get Energy
Modify

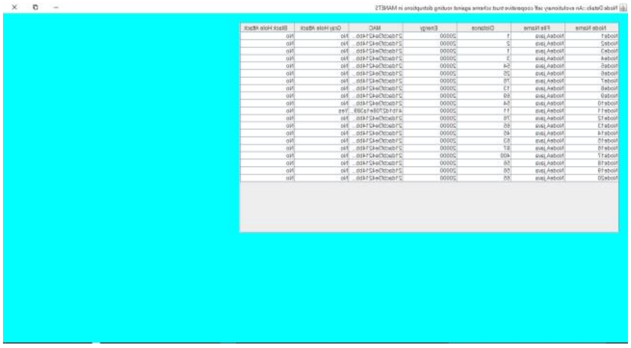
Gray Hole Attack :

It is one of the routing disruption attacks, using which the attacker can add the Malicious Data to the particular node.


Gray Hole Attack(Packet Dropping) :: An evolutionary self cooperative trust scheme against routing distruptions in MANETS
Select Node
Node9
Malicious Data
Attack

Node Details :

This Screen shows all the Nodes Details covering from Source to Destination node.


Node Details ::An evolutionary self cooperative trust scheme against routing distruptions in MANETS

Node Name	File Name	Distance	Energy	MAC	Gray Hole Attack	Black Hole Attack
Node1	NodeA.java	1	20000	[illegible]	No	No
Node2	NodeA.java	2	20000	[illegible]	No	No
Node3	NodeA.java	1	20000	[illegible]	No	No
Node4	NodeA.java	3	20000	[illegible]	No	No
Node5	NodeA.java	45	20000	[illegible]	No	No
Node6	NodeA.java	52	20000	[illegible]	No	No
Node7	NodeA.java	67	20000	[illegible]	No	No
Node8	NodeA.java	31	20000	[illegible]	No	No
Node9	NodeA.java	96	20000	[illegible]	No	No
Node10	NodeA.java	45	20000	[illegible]	No	No
Node11	NodeA.java	11	20000	[illegible]	Yes	No
Node12	NodeA.java	67	20000	[illegible]	No	No
Node13	NodeA.java	66	20000	[illegible]	No	No
Node14	NodeA.java	54	20000	[illegible]	No	No
Node15	NodeA.java	36	20000	[illegible]	No	No
Node16	NodeA.java	78	20000	[illegible]	No	No
Node17	NodeA.java	400	20000	[illegible]	No	No
Node18	NodeA.java	65	20000	[illegible]	No	No
Node19	NodeA.java	65	20000	[illegible]	No	No
Node20	NodeA.java	66	20000	[illegible]	No	No

VI. CONCLUSION

In this paper, we propose a self-cooperative trusting nodes (SCTN) scheme to resist against various routing disruption attacks. SCTN mimic human cognition process and promotes the attribute of network scalability and also ensures reliable routing in MANETs using a step process. Firstly, it uses a detection mechanism to identify the trustworthy of nodes. Secondly, it uses cooperative mechanism to share the trust information among the network nodes and Thirdly, it dynamically changes the network topology to protect its significant data from the malicious nodes.

VII. FUTURE ENHANCEMENT

As further enhancement, we could use adaptive transmission intervals for Hello messages to be sent from benign nodes to identify the malicious node very quickly.

REFERENCES

[1] Z.Movahedi et al, “Trust Distortion Resistant Trust Management Frameworks on Mobile Ad hoc Networks: A Survey,” IEEE Communications Surveys & Tutorials, vol.18, pp.1287-1309, 2016.

[2] Y.Wu,Y.Zhao, M.Riguidel, G. Wang, and P.Yi, “Security and trust management in opportunistic networks: a survey,” Security and Commn. Networks, vol 8, pp.1812 – 1827, 2015

[3] Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," IEEE Communications Surveys & Tutorials, vol. 15, pp. 2027-2045, 2013.

[4] A.A. Pirzada et al, “Secure Routing protocols for Mobile Ad hoc Wireless Networks,” in advanced wired and wireless Networks, Boston, MA: Springer US,pp.57-80.

[5] P. Zhou et.al, “toward energy efficient trust system through watchdog optimization for WSNs”, IEEE Transactions on Information Forensics and security, vol.10,pp. 613-625.

BIOGRAPHY

Dr. R. Rajani is a Professor and heading the department of MCA, Narayana Engineering College, Nellore, AP, India.
She guided many projects for both B.Tech and PG Students. Her research interest include Data Mining, Data Science, Computer Networks and Software Engineering etc.,

SK. Asia is currently pursuing her Post Graduation (Master of Computer Applications) in Narayana Engineering College, Nellore affiliated to JNTUA University, Andhra Pradesh, India. She had a membership in CSI (Computer Society of India).

G. Bhagya Lakshmi is currently pursuing her Post Graduation (Master of Computer Applications) in Narayana Engineering College, Nellore affiliated to JNTUA University, Andhra Pradesh, India. She had a membership in CSI (Computer Society of India).