Modified- Secure Collaborative Trust Based Approach for Wormhole Attack Elimination MANET

Prepared by,
S.Darsni
S.Naveena
G.Jagadheeswari
M.Swetha

Guided by,
Mrs.M.Sathya Priya.M.tech.,Assistant professor
Department of computer science engineering.

Objective

To eliminate the Wormhole Attacker collusion occurred by the two or more devices communicating via optimal relay with centralized router using MANET network.

The overall delay and Energy Usage is reduced with increase in throughput.

Abstract

Eliminate the Wormhole Attacker occurred by the two or more devices communicating via optimal relay with centralized router using MANET network.

The overall delay is reduced with increase in throughput.

This project studies the important of wireless communication under Wormhole Attacker Detection where detecting the dropper node.

Introduction

In MANET, the participating node has a limited transmission range.Therefore, two nodes will not be able to communicate With each other if they are not in the range of radio coverage of each other.

Thus, the transmission through multi-hops scenario will be employed and the intermediate node has to forward the packet to the next node until it reaches the destination.

Software requirements

Programming language:python,tcl
Processor:1.4 GHz Pentium IV
Operating system: linux,windows
Ram:4 GB
Hard drive:500 GB
Tools:Ns-allinone-2.28
Pre-request software:Cygwin

Existing system

The wormhole attacks is very challenging issues and one of the serious security threatsin detection to MANET.

Existing proposed a novel HWAD secure algorithm for wormhole detection in MANET.

HWAD reduce the delay and energy through avoids performing wormhole detectionsfor all available nodesin the network

Disadvantages of existing system

However, a HWAD strategy usually gives rise to large-scale wireless signal collision and interference since it increases the number of messages transmitted in the network.

Incur high delay delivery, or fail to provide high throughput,packet delivery ratio as well as consume higher energy

Proposing system

In this project, we select any node as the source node from participant node in a network.

To use cache block list, we select all intermediate node for message passing via that node Route request send to all intermediate node by source node. If it is get the route request packet then give response for that route request packet.

Proposing system

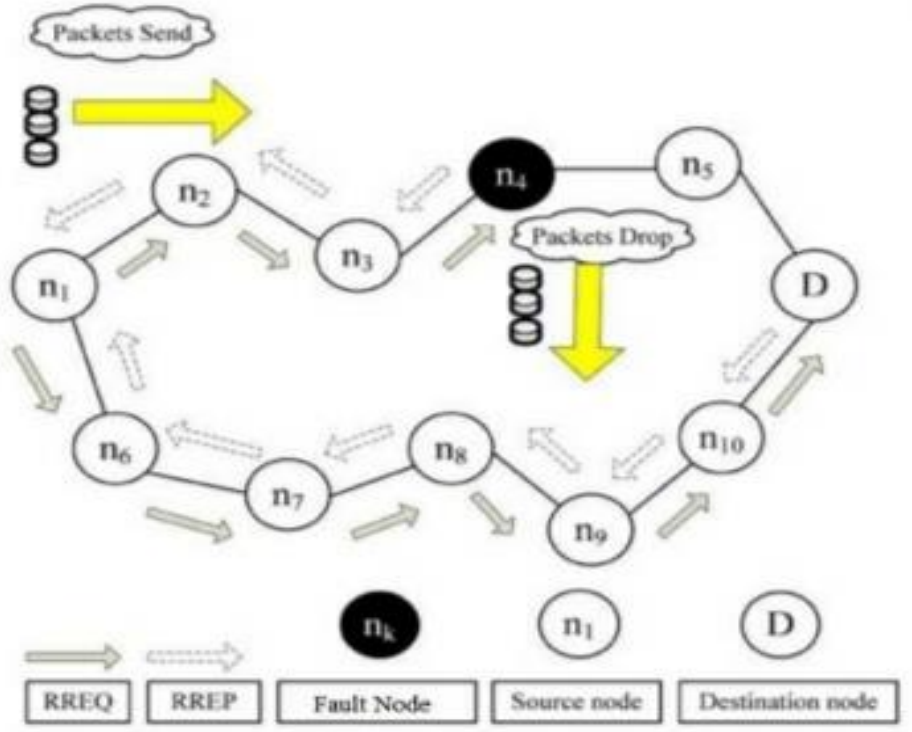
When the source node received the route response packet then its move to Collaborative Trust algorithm, which is used to detecting the dropper node .

Which is split the node into two type

One is no dropper node and another one is dropper node.

If the node is No dropper type which is move to destination then raise alarm for detecting dropper node

Methodology



Advantages of proposed system

In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detectionmechanism again.

This function assists in sending the bait address to entice the dropper nodes and to utilize the reverse tracing program of the Wormhole Attacker to detect the exact addresses of droppernodes.

Expected results

Packet Delivery Ratio: It is defined as the ratio of the number of the number of packets sent by the source to the packets received at the destination.

Average End-to-End Delay: It is well-defined as the average time taken for a packet to be transmitted from the source to the destination.

Throughput: It is defined as the total amount of data, that the destination receives them from the source which is divided by the time it takes for the destination to get the final packet.

References

[1] S. Majumder and D. Bhattacharyya, ‘‘Mitigating wormhole attack in MANET using absolute deviation statistical approach,’’ in Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC), Las Vegas, NV,USA, Jan. 2018, pp. 317–320.

[2] J. Seo and G. Lee, ‘‘An effective wormhole attack defence method for a smart meter mesh network in an intelligent power grid,’’ Int. J. Adv. Robot. Syst., vol. 9, p. 49, Dec. 2012.

[3] S. Amutha and K. Balasubramanian, ‘‘Secured energy optimized ad hoc on-demand distance vector routing protocol,’’ Comput. Electr. Eng., vol. 72, pp. 766–773, Nov. 2018.

[4] S. Rezaei, M. Gharib, and A. Movaghar, ‘‘Throughput analysis of IEEE 802.11 multi-hop wireless networks with routing consideration: A general framework,’’ IEEE Trans. Commun., vol. 66, no. 11, pp. 5430–5443, Nov. 2018, doi: 10.1109/TCOMM.2018.2848905.

[5] M. Zaminkar and R. Fotohi, ‘‘SoS-RPL: Securing Internet of Things against sinkhole attack using RPL protocol-based node rating and ranking mechanism,’’ Wireless Pers. Commun., vol. 114, no. 2, pp. 1287–1312,Sep. 2020.

Thank you