ISSN: 0974-5823 Vol. 6 No. 3 October-December, 2021

International Journal of Mechanical Engineering

Security in Mobile Ad hoc Network based on Secure Zone Routing Protocol

K. R. Kannan*
Assistant Professor, Hindusthan Institute of Technology, Malumichampatti, Tamil Nadu 641028, India.
Mail Id: kannan.kr@hit.edu.in

Dr. C. N.Marimuthu
Professor and Dean, Nandha Engineering College, Erode, Tamil Nadu 638052, India.

R K Arunkumar
Assistant Professor[3], Nandha College of Pharmacy, Erode, Tamil Nadu 638052, India.

Abstract:

A Mobile Ad hoc NETwork or MANET is a kind of ad hoc network that will be able to change locations and configure itself on the run. MANET does not require any fixed infrastructure or central control system. This means the nodes can interact any time with the network. The processing capacity of all the nodes must be equal. The security aspect in ad hoc network is based on the use of a proper key management system. These networks differ from one another in many aspects. It also needs environment-specific and efficient key management system. Secure routing protocols in ad hoc networks are designed to counteract routing attacks that disrupt route discovery. The prominence of planned key is, Secure Zone Routing Protocol (SZRP) which guarantees safety as wanted by affording a complete construction based on well-organized safe neighbor discovery, protected routing packets, recognition of spiteful nodes and precluding the devices from extinguishing the system. Both effective key management and secure neighbor mechanism are used to achieve the objective.

A. INTRODUCTION

An Ad hoc Network is a Wireless Mobile Mesh Network encompassed of two or more devices fortified with wireless communications and networking ability. Every connected device in a MANET moves independently in any direction and hence often changes its links to other devices. The main criterion in building a MANET is enabling every device to continuously maintain the data required to route the traffic properly. The advantage of minimum configuration and easy deployment make these networks suitable for emergency conditions such as natural disasters or man-made conflicts. Ad hoc networks can be formed quickly by the presence of dynamic and adaptive routing protocols. Further ad hoc network can be further classified by their applications.

MOBILE AD HOC NETWORK (MANET)

MANET is a mobile wireless network consisting of mobile computing systems that use wireless transmission for interacting with each other without any established infrastructure. Interference and hence connectivity is determined by the network topology. The mobility layout of the mobile devices in the network will impact its performance which may require for the data to be resent frequently. Also, distribution of resources in the network like power remains unclear. The application for MANET is many ranging from mobile, highly dynamic networks, large-scale to static and small networks which are restricted by power sources. A comprehensive security for network should have inhibition, finding and response.

B. ALLIED WORKS

The most fundamental research issue in MANET is routing and must deal with constraints such as low bandwidth, high power consumption, high error rates and unpredictable movements of nodes. Each layer is subjected to attacks, which can be at two levels one is at routing level and other is to destroy the security mechanism used in network. Attacks are of two types they are active and passive attack. In MANET, any number of nodes can freely join or leave the network. This is called the open network boundary. This poses challenges in security against harmful activities to nodes in MANET. The goal of the work is to provide key management with resource constraint. The Public key management system support secure communication based on certificate based schemes during authentication. The requirement of any security needs a hope based model .A key management system and cryptography are used to provide security [1].The Mobility increases the complexity. A trust based language analysis of OLSR protocol is used to identify the characteristics of unruly nodes and a solution is proposed [2]. A simple routing algorithm is the one in which each incoming packet is sent through every outgoing link except in the one in which it arrived. Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols including OSPF, DVR. Bandwidth and memory consumption are two factors for key management. A Conviction based scheme called Enhanced OLSR (EOLSR) to safe guard devices against attack. The technique is used to find whether the node is providing correct information. The advantage is it has no high calculation [3]. This topology information is used by individual nodes for computing subsequent hop destinations for all nodes in the network using shortest hop forwarding paths. OLSR depends on multipoint relay (MPR) choice which impacts the routing protocols performances, the overhead generated by the OLSR protocol and more specifically the flooding efficiency depend on MPR selection. MPRs become intermediate nodes in the routes. Spoofing is a major problem in routing, [4] devised a LT-OLSR protocol to protect network against attacks. A routing Table integrity is maintained in network. The core aspects to protect ad hoc network are path accessibility, secrecy, data integrity, authentication and non-repudiation. The network consists of unreliable wireless link among the nodes, where the power supply is limited for wireless node and the mobility of the node. The routing data is rehabilitated due to the nodes strength. A selection process is suggested [5] to minimize unwanted broadcast using modified MPR set to defend node on attack named DFOLSR. The Multipoint Relays (MPRs) which are selected nodes responsible to forward messages.

In route discovery [11], a route request packet is sent by the node to initiate route discovery. When the Route Request packet arrives at the destination node, the destination node checks the originator identity before replying. OLSR figures a selected router on each link to perform flooding of topology information. A specific method [7] is required in order to best optimize the flooding process. Nodes choose MPRs in a way that there is a route to each of its hop neighbors, MPR nodes then source and send TC messages that contain the MPR selectors. OLSR, which follows hello and topology control communications to discover and then propagate link state information all through the network. Two methods [6] are presented for attacks against OLSR. Prevention resolves protocol vulnerability, counter measures that react to misbehavior and inconsistency. Elliptic curve cryptography as a public key cryptography for mobile environment Elliptic Curves offers security to classical systems, with fewer bits. Elliptic Curves implementation in cryptography can be done with smaller chip size, little power utilization, better speed. Elliptic Curve Cryptography is stronger than RSA for key sizes it offers an alternative to RSA and DSA. ECC are relatively convenient to function and extremely difficult to reverse. Key exchange protocol such as Diffie–Hellman (DH) Algorithm assists two devices interacting over public channel to reach a mutual secret without being transmitted. DH practices two public key to encrypt and decrypt their conversation. Specification-based intrusion detection [9], is the one in which manually designed program behavioral specifications are utilized as a platform to determine attacks. This is offered as an important alternative that can group the advantages of misuse detection and anomaly detection. IDS implements two methods of intrusion detection which are signature-based intrusion detection and anomaly-based intrusion detection. Signature-based intrusion detection helps to determine probable attacks by studying the traffic of a given network along with its log data to existing attack patterns, a malleable approach to manage threats. [13] Luus–Jaakola (LJ) search is experimental global optimization for a real valued function, a proper iterative method that generates a sequence. For each iteration, the neighborhood decreases which forces a subsequence to converge to a cluster point. An active attack [10] is an exploitation of the network where a threat is attempted to make changes to data on the target. Active Attack is danger for integrity and availability. Point detection for single attack and IDS for varied range of attack. Network layer attacks can block completely the services of the wireless network and they can fabricate the packets transmitted between devices on the network. RS codes are used to correct errors in storage devices. The algorithm [12] reduces complexity in data communication. One way hash fashion has low computation overhead and memory overhead is a better option to protect against false injection. An intrusion detection system [8] (IDS) checks a network for any malicious activity. The violation in the network is grouped centrally using a security information and event management system. MANET is well recognized to various attacks due to their arrangement and energy. The system to sense unexpected attacks and segregate intruders.

C. SECURE ZO NE RO UTING P RO TOCOL

The underlined goals are required for the MANET planned design:

□□□Few Procedural steps are needed to back up power for all devices else the battery be trenched.

□ Support secure routing ,operative key administration

□ Address security concern like end to end authentication, message integrity and data confidentiality

□ Less retention, processing power and trusted certification authority

C.1 SAFE NEIGHBOR DISCOVERY

In wireless networks, Neighbor discovery protocol allows various nodes on the same link to communicate their presence to the neighbors and to find about the presence of their neighbors, which uses messaging to handle the communication between neighbor nodes. Neighbor Discovery determines half-link catastrophes by using neighbor unreachability detection. Neighbor Discovery prevents sending traffic to neighbors when two-way connectivity is not present.

C.2PROTECTED ROUTING PACKETS

Routing and data messages are two security facilities in MANET. The messages have a sundry nature and dissimilar security needs. Routing creates the fundamental communication between networks, makes an addressing pattern that uniquely identifies every system and organizes individual systems into a hierarchical network layout. It is important to focus on message routing where messages are routed from producers to routers. This message from the router is then routed by the router based on the message's address and routing pattern. The route taken by the data packets for reaching a particular destination is referred as data routing. Data packets will be re-sent while they are being dropped but also implemented to vacant spots in data resulting in creating complete information.

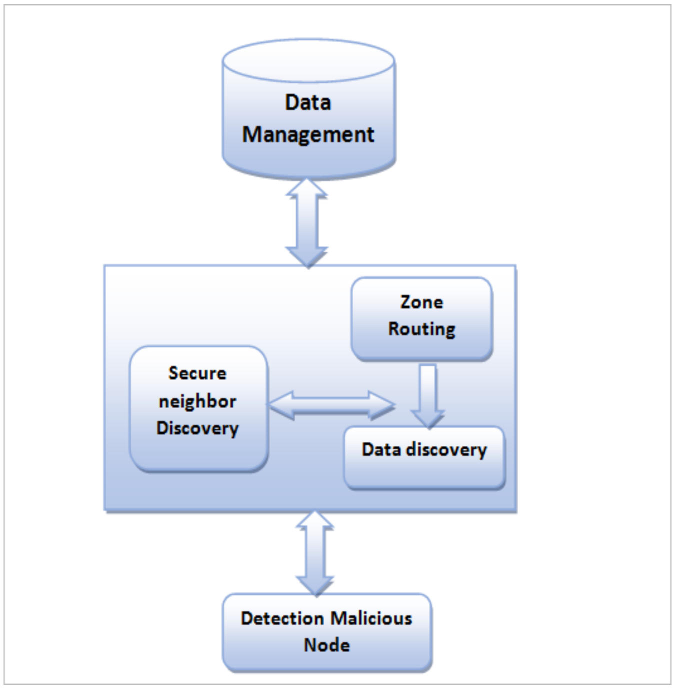


Fig.1 Work Flow Design

D.IMPLEMENTATION

□ The 35 nodes are imitated for SZRP which extent arbitrarily, the broadcast is random for all devices.
□ Devices were situated on any direction. The range for each broadcasting device move randomly to an arbitrary path with an unsystematic energy.

Device Formation

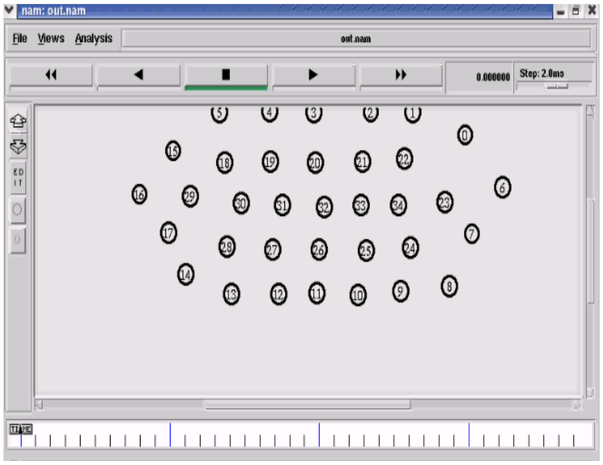
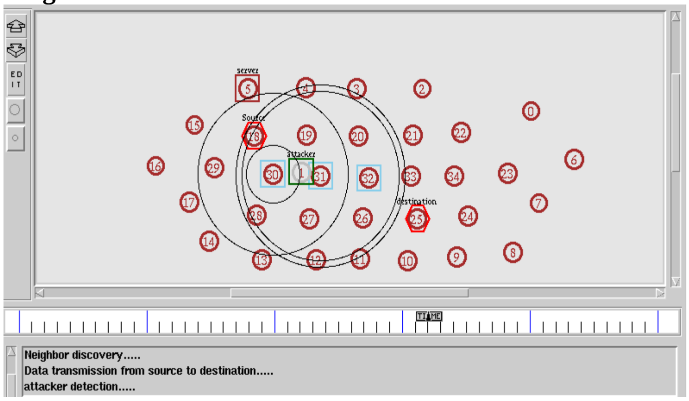


Fig.2 Device Formation

The device is made to move in 3D Structure. The third direction is not castoff. The device is made to move horizontal. So the nodes 3D structure is altered based on device dynamics.

Neighbor Determination and Data Broadcast

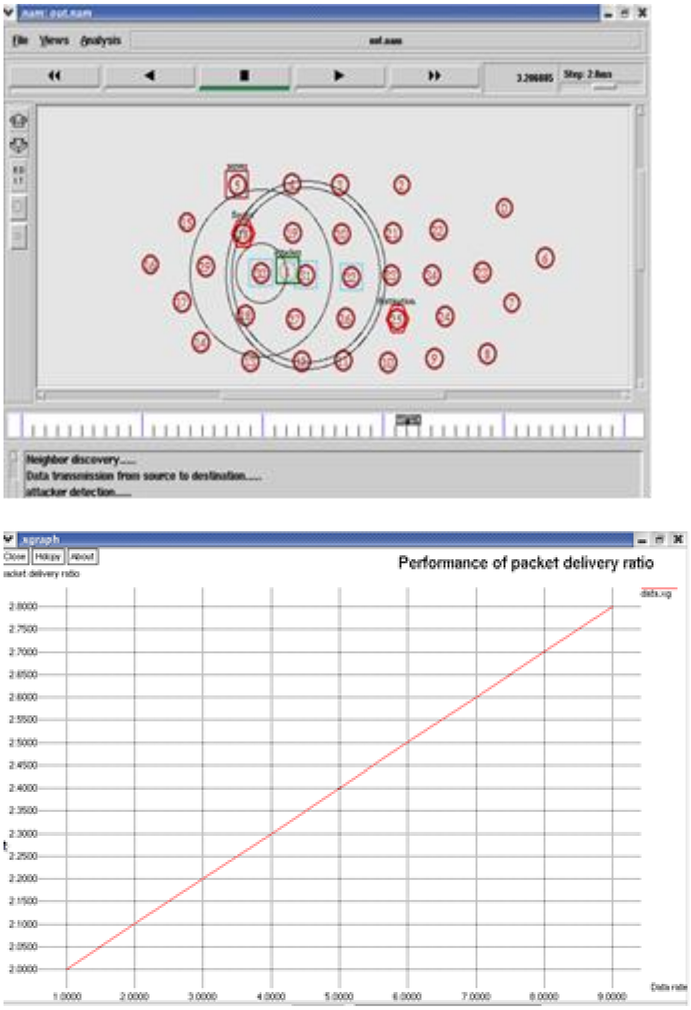


Neighbor discovery.....
Data transmission from source to destination.....
attacker detection.....

Fig 3 Neighbor Determination and Data Broadcast

The System includes Safe neighbor locality, protected routing packets, finding and avoiding the spiteful devices from rescinding the system. Besides the broadcast the route at every hop is calculated as one transmission.

Outcome of Spiteful Node



Neighbor discovery.....
Data transmission from source to destination.....
attacker detection.....

Fig.4 Outcome of Spiteful Node

The Packet Delivery Ratio (PDR) of low dynamic network increases as speed increases but the travel route never changes. So this accomplishment will increase Packet Delivery Ratio and find the outcome of spiteful node.

E.CONCLUSIONS

Zone Routing Protocol is unswerving to contrivance the safety which highlights the glitches and routing in open terrain. The protocol is strong for manifold incidences and was planned to the perseverance.

F.REFERENCES

[1]. M. Omar, Y. Challal, and A. Bouabdallah, " Reliable and fully distributed trust model for mobile ad hoc networks ," Computers & Security, vol. 28, pp. 199 – 214, 2009.

[2]. A. Adnane, C. Bidan, and R. T. de Sousa Júnior, "Trust - based security for the olsr routing protocol," Computer Communications , vol. 36, no. 10, pp. 1159–1171, 2013

[3]. M . Marimuthu and I. Krishnamurthi, "Enhanced olsr for defense against dos attack in ad hoc networks ," Communications and Networks , Journal of, vol. 15, no. 1, pp. 31–37, Feb 2013.

[4]. Y. Jeon, T.-H. Kim, Y. Kim, and J. Kim, " Lt -olsr: Attack-tolerant olsr against link spoofing," in Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks (LCN 2012), ser. LCN '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 216–219.

[5]. D. Malik, K. Mahajan, and M. Rizvi, "Security for node isolation attack on olsr by modifying mpr selection process ," in Networks Soft Computing (ICNSC), 2014 First International Conference on, Aug 2014, pp. 102– 106.

[6]. A. Adnane, C. Bidan, and R. de Sousa, "Trust-based counter measures for securing olsr protocol," in Computational Science and Engineering, 2009. CSE '09. International Conference on, vol. 2, Aug 2009, pp. 745– 752.

[7]. P. Suresh, R. Kaur, M. Gaur, and V. Laxmi, "Collusion attack resistance through forced mpr switching in olsr," in Wireless Days (WD), 2010 IFIP, Oct 2010, pp. 1–5.

[8]. A. Nadeem and M. Howarth, " Protection of manets from a range of attacks using an intrusion detection and prevention system," Telecommunication Systems , vol. 52, no. 4, pp. 2047–2058, 2013.

[9]. A. Nadeem and M. P. Howarth, "An intrusion detection & adaptive response mechanism for manets ," Ad Hoc Networks , vol. 13, Part B, no. 0, pp. 368 – 380, 2014.

[10]. A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," Communications Surveys Tutorials, IEEE, vol. 15, no. 4, pp. 2027–2045, Fourth 2013.

[11] Upendra Roy B.P., Rengarajan N., "Feasibility Study of an Energy Storage System for Distributed Generation System in Islanding Mode", Journal of Energy Resources Technology, Volume 139, Issue 1, January 2017.

[12] Deepa A., Marimuthu C.N., "Modified RS encoder architecture with reduced critical path delay for high speed data communication Proceedings of the International Conference on Intelligent Sustainable Systems, ICISS 2017, Pages 617-620, June 2018

[13] Murugesan C., Marimuthu C.N., "Cost optimization of PV-Diesel Systems in Nanogrid Using L J Cuckoo Search and its Application in Mobile Towers", Mobile Networks and Applications, Volume 24, Pages 340-349, April 2019.