Secure Routing Protocol against Internal and External Attack in MANET

Nitesh Ghodichor[1], Raj Thaneeghaivl. V[2], Varsha Namdeoe[3], Gautam Borkar[4]

{niteshgho@gmail.com[1],rajthaneeghavelv@gmail.com[2],varshanamdeo@yahoo.com[3], gautamborkar2@gmail.com[4]}

CSE, SRK University, Bhopal, India[1, 2, 3], RAIT, Mumbai University, Mumbai, India[4]

Abstract. A mobile ad-hoc network is a group of mobile nodes that connect with one another via wireless networks to build a temporary network without the use of infrastructure or centralized administration. Secure routing is an important concern in MANET. This paper discusses the existing routing protocol in MANET, security issues while routing, and the existing secure routing protocol. The second part of the paper focused on a proposed secure routing algorithm (SRA) that provides security by employing an anonymous key establishment method that avoids the involvement of malicious nodes in routing. In MANET, the secure routing protocol protects the network from both internal and external attacks.

Keywords: MANET, Wireless Network, Security, Attacks and Malicious Nodes, Secure Routing, security mechanism.

1 Introduction

MANET is a network of wireless nodes that travel between nodes to construct a network structure without relying on infrastructure or a central administrator. MANET is the most often used network due to its ease of installation. In a MANET, information is transferred from one node to another via radio frequency, which is referred to as peer to peer communication. MANET is extremely vulnerable to assault due to its open nature. The attacker may attack the network while data or packets are being transferred from one node to another, and it may also observe the network's activity before the attack. There are two sorts of assaults: data traffic attacks and control traffic attacks.

In MANET, control information is transferred first to maintain the network operational, followed by original data for communication, which is sent in the form of packets. Attackers may target either one or both; an attack is defined as any activity that compromises the network's security or any threat that compromises the network's security information. MANET security is a primary concern. Establishing an end-to-end link in open media is extremely tough. To ensure security, many security mechanisms and protocols have been established. Authentication is accomplished through the use of key-based protocols and an IDS system. It is critical to secure the suggested plan. Secure Routing Protocol ensures the security of MANET networks by

THEETAS 2022, April 16-17, Jabalpur, India

DOI 10.4108/eai.16-4-2022.2318163

utilising an anonymous key establishment and route finding method that prevents nodes from becoming malevolent.

2 Routing Protocol in MANET

Due to the nomadic nature of the network's nodes, routing is a critical topic in MANET. To route the packet from source to destination, it is critical to determine the path. It is critical to build a path between source and destination in a mobile environment and to maintain that path for safe communication. In MANET, there are primarily two types of routing protocols.

2.1 Proactive Routing

Proactive routing protocols preserve network connectivity by maintaining information on all routes. Control packets are sent regularly to ensure network connectivity. Thus, packets are sent on a regular basis and the routing table is maintained. The proactive routing protocol locates and maintains its route using the link state routing algorithm. The proactive routing protocols are DSDV and OLSR.

DSDV

The destination sequenced distance vector routing protocol is based on the Bellman-Ford algorithm. It is a hop-by-hop vector routing system. Each routing table comprises a list of all accessible destinations, as well as the number of hops required to reach each. Each entry is assigned a sequence number, which aids in recognising it. This approach enables the protocol to prevent routing loops by requiring each mobile node in the network to advertise its own routing table to its current neighbour on a frequent basis. Advertising is distributed via broadcast or multicast. Through advertisement, the neighbouring node can learn about any changes in the network caused by its movements. Two methods are used to update the routing table. a) Full Dump: the neighbours receive the entire entry routing table. b) Incremental updates: only the entries that require modification are transmitted.

OLSR

In OLSR, message flooding is minimised through the use of multipoint relaying (MPR). Each node N in the network selects a set of neighbour nodes as a multipoint relay, MPR(N), which transmits control packets from N neighbours but does not forward them. MPR (N) is chosen since it encompasses all of N's two-hop neighbours (N). Because OLSR has a shorter end-to-end delay, it is ideal for applications requiring a minimum of delay. The primary downside of OLSR is that it maintains routing tables for all possible routes, which means that as the number of mobile hosts increases, the overhead from control messages increases as well, requiring more processing resources than other protocols when discovering another route.

2.2 Reactive Routing

Reactive routing is a type of on-demand routing protocol in which control packets are sent only when the source node requires communication with the destination node. Reactive routing is a bandwidth-efficient routing technique that utilises on-demand transmission to conserve network bandwidth. Additionally, it reduces the overhead associated with proactive routing. It establishes a route between the source and destination nodes using the distance vector routing technique. AODV, DSR, and TORA are all protocols for reactive routing.

AODV Routing

The ad-hoc on-demand distance vector (AODV) protocol establishes a route between sources and destinations fast and efficiently because it is not required to maintain the route to the destination while communication is not active. When a route to the destination is required, the node broadcasts an RREQ, which is received by the destination node on an intermediate node. [19]. The route is enabled by unicasting an RREP back to the RREQ source. The route that has expired is indicated by an invalid status in the routing table item.

DSR

Dynamic Source Routing is a reactive protocol that is based on source routing. When a source node wishes to send a packet, it instantly begins searching the routing table for the needed sink. When the source discovers alternative routes, the one with the fewest hops is chosen and appended as a header to the transmitted data packet [20]. During the route discovery process, RREQ messages are flooded into the network. Each node receives the RREQ packet and verifies the destination node's availability. As soon as the destination node receives the RREQ packet, it instantly sends the RREP packet to the source node.

TORA

Temporarily Ordered Routing Algorithm is an on-demand routing protocol that determines the best route from source to destination using Directed Acrylic Graf (DAG). TORA necessitated complete network synchronisation. TORA prevents control messages from propagating throughout the network. TORA supports multipath routing, which is a method of transmitting data packets from source to destination using multiple routes. Through the use of three distinct phases: a) route creation, b) route maintenance and c) route erasure.

Route Creation: It is the process of connecting sources to destinations using a DAG-based algorithm based on known heights; a node with a lower height is downstream, while a node with a higher height is upstream.

Route Maintenance: It is the process of responding to changes in the network's topology in such a way that the route to the destination is reestablished in a finite amount of time.

Route Erasure: It is the process of remaining invalid route from the network if ant partition detected in the network the directed route.

3. Security in MANET

Security is a critical consideration in MANETs. Due to the open nature of MANET, it is extremely vulnerable to attacks. An attack is defined as an unauthorised action within the network that disrupts the operation of the network. Different types of attacks are defined in MANET as follows:

Wormhole attack: In a wormhole attack, the attacker creates a tunnel between two malicious nodes and uses the tunnel to route packets from one point to another.

***Hello flood attack**:* When a node in the network broadcasts the hello packet at a high rate, this is referred to as a hello flood attack. As a result, each node in the network determines that this is the optimal route to the destination and selects the route that results in packets reaching the attacker node [1].

***Man in Middle attack**:* For a man-in-the-middle attack, the attacker node must enter between two users' conversations, interrupt them, or alter their communication. For a man-in-the-middle attack, the attacker node must become the network's path.

***Bogus Registration Attack** :* In this attack, the attackers pretend to be another node either by sending stolen beacons or by generating such false beacons in order to register as a neighbour with a node. Once registered, the attackers may completely disrupt the network.

***Rushing Attack**:* This is referred to as a network layer attack. In this attack, the attacker node receives the RREQ packets and immediately forwards them without processing them to its neighbours. Rushing attacks take advantage of redundant suppression mechanisms. A rushing attack expedites the transmission of a malicious RREP on behalf of another node, bypassing any necessary processing.

***Blackmail Attack**:* Blackmail attacks occur when attacker nodes falsely accuse an innocent node of being a malicious node. This attack is effective against distributed procedures that generate a list of good and bad nodes based on a review of MANET's participating nodes. Attackers transmit invalid RREP messages with ads to particular nodes at an unreasonably high cost [1].

***Cache Poisoning Attack**:* Each route maintains a small number of transmission routes until each entry reaches a timeout. As a result, each route exists in the node's memory for a brief period of time. If a malicious node launches a routing attack, the malicious node's routes will remain in the node's route table until a timeout occurs or a better route is discovered. It can advertise itself as a route to a remote node that it is unable to reach. Once included in the path, the attacker node is free to carry out its malicious behaviour [1].

***Sybil Attack**:* Sybil attacks occur when a single node in a network adopts many identities simultaneously. It introduces complications while attempting to connect to a peer-to-peer (P2P) network. By manipulating the network, it develops bogus identities and gains control of the entire system. All of these identities appear to be normal users, however, they are all associated with a single entity, an unknown user referred to as an attacker. It intercepts routing messages and wreaks havoc on the operation of the network.

***Black hole Attack**:* In a black hole attack, a malicious node simulates a black hole, obliterating all data packets that pass through it, just as all energy in the universe vanishes. The attacker node partitions the network into distinct segments.

***Gray hole Attack** :* The attacker node drops the packet, but the node's harmful activity is limited for a specified amount of time as a result of this behaviour [1]. It is classified into two categories: a) An assault that is node-dependent; b) An attack that is time-dependent

Node-dependent: packets going for or originating from a single victim node are dropped. While the remaining nodes operate normally, correctly routing data packets to the destination node.

Time-dependent: discard packets only for a certain time period when forward data packets are regularly sent.

***Jellyfish Attack**:* Rather of discarding the data packet, the attacker delays its delivery in this case. It randomly scrambles the order of the packets that received the original packet. As a result, the typical flow mechanism is interrupted. Jellyfish is in charge of packet transfer from end to end.

4. Secure Routing Mechanism in MANET

To ensure network security in MANET, a variety of secure routing mechanisms have been devised and utilised. We cover many secure routing mechanisms in this study, including key-based routing, intrusion detection systems, and watchdog processes.

4.1 Key Based Mechanism

Key management is the fundamental technique for MANET security. Secure key management and encryption ensure that communication nodes have a public / private key pair or symmetric key pair.

Group key management

It is used for multicast communication, a very efficient method of communication for group applications like as video conferencing. To ensure multicast communication, a collection of keys should be shared across all group members. According to M. EL Bashary et al., a group key should be exchanged amongst all group members for multicast communication. With the group key, only an approved user should be able to encrypt or decrypt the data. However, owing to the nature of MANET, it is possible for a group member to be altered. The group gains a new member. It is necessary to produce a new group key and distribute it to all group members. It stops new group members from accessing previously transmitted group information. Two protocols are used to maintain group keys [18]**.**

Centralized group key management protocol: In this protocol, a single key server is responsible for the production, distribution, and update of the group key.

Decentralized group key management protocol: Key management is not centralised. It is used to enable highly scalable key distribution by dividing the cluster into subgroups that are maintained by the cluster heads.

4.2 Intrusion detection System (IDS)

An intrusion detection system (IDS) monitors the system for suspicious behaviour. When it is necessary to identify suspicious behaviour in the network, each mobile node works as an IDS agent. The node detects local incursion, collaborates with its neighbouring node, and then decides on the optimal approach. There are three distinct types of IDS techniques: standalone, cooperative, and cluster-based.

Zing et al. (2007) described the fundamentals of IDS approaches, stating that each node in an ad-hoc network is an IDS system. It anonymously recognises processes and detects local intrusions, and while routing, a collaborative process occurs.

4.3 Watchdog Method

It is used to identify node misbehaviour by copying packets into buffers and observing how neighbouring nodes respond to these packets. When a node transmits a packet, the node's watchdog verifies that the packets are likewise forwarded by the subsequent nodes in the route. According to Gupta et al., the watchdog snoops promiscuously to determine whether or not the next node sends the packet unchanged. A packet that remains in the buffer after the timeout period without a successful match is identified as dropped or changed, and the node that passes it is deemed suspicious or malicious.

5. Proposed Scheme

A scheme that is being proposed A secure routing protocol guards against assaults in a MANET. A network's security is provided by an implementation module through the use of anonymous key establishment between two communicating nodes and a secure route discovery mechanism from source to destination. It prevents hostile nodes from joining the network and also prevents network nodes from becoming malevolent, hence producing a completely secure network for transmission.

Anonymous key establishment: Each node engaged in packet transmission establishes a session key with its neighbouring node for each session during packet transmission. It is a shared secret key, and transmission will commence only when both parties have authenticated the key [4].

Secure route discovery: The route finding procedure is carried out anonymously. The source node initiates the secure route establishment process to the destination node using the shared secret session key [4].

According to the suggested technique, if any node in the network becomes hostile, it is unable to calculate the shared secret key required for data transfer, and any node from the outside is prohibited from entering the network without first calculating the shared secret key. This technique ensures security on a number of fronts, including privacy protection and packet delivery ratio or throughput.

6. Expected Outcome

When compared to the AODV routing protocol, the suggested scheme "Secure Routing Protocol for MANET" achieves. Because the suggested protocol is a privacy-protecting routing protocol and AODV is the sole routing protocol that is unable to guarantee security while routing, packets are dropped more frequently in AODV than in a secure routing protocol. It has an effect on the network's throughput. As a result, the secure routing protocol's projected throughput is larger than that of the AODV routing protocol. The methods described will be executed for a certain setup. NS3, Random Node Placement, 50 Nodes, and Multicast Routing.

7. Conclusion

MANET is composed of autonomous mobile nodes. It is a self-configuring mobile ad hoc network with an embedded self-configuring and self-organizing network. MANET eliminates the need for centralised or fixed infrastructure by allowing nodes to interact directly with one another. MANET operation and use of the routing protocol inside the network involves registering and configuring him in the network in order to initiate information exchange with all neighbour nodes for the purpose of updating the routing table and other required information. While data transmission and control within the network are dynamic, any invalid node that gains access to data or control over their path as a result of an attack on control messages loses the packet or disrupts the network as a result of the attacker.

We will explore several attacks that result in message dropping and the execution of all bogus transmissions and conversations in this section. Existing routing mechanisms in MANET and AODV are muddled and perform erratically during communication. Each type of attack has an effect on and eavesdrops on the network via faulty nodes, bloated networks, tunnelling across pathways, and packet dropping attacks. This always results in a change in network behaviour as a result of an attack. MANET's secure routing system safeguards users' privacy and significantly enhances packet delivery ratios.

References

[1] Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose, Himadri Nath Saha, Debika Bhattacharjee: Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques, November 2011

[2] Mohamed A. Abdelshafy, Peter J. B. King: Resisting Blackhole Attacks on MANETs,2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)

[3] V Patil, P Fulare, N Ghodichor: An Unobservable Secure Routing Protocol with Wormhole Attack Prevention for Mobile Ad-Hoc Network, International Journal of Current Engineering and Technology E-ISSN 2277–4106, Vol-4, No.-3,2014 PP 1930-1932

[4] V Patil, P Fulare, SS Patil, N Ghodichor: A Review on an Unobservable Secure Routing Protocol with Wormhole Attack Prevention in Manet, IOSR-JCE, E-ISSN: 2278-0661, 2014, PP 16-19

[5] Usha and Bose: Comparing the Impact of Black Hole and Gray Hole Attacks in Mobile Adhoc Networks, Journal of Computer Science 2012, 8 (11), 1788-1802

[6] Aakanksha Kadam, Niravkumar Patel, Vaishali Gaikwad: Detection and Prevention of Wormhole attack in MANET, IRJET, Volume 03, Issue 03, Mar-2016,pp-388-393

[7] Arathy K Sa, Sminesh C Na A: A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET, Government Engineering College Thrissur, Kerala, 680009, India Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016)

[8] Kishor Dongarwar, Nitesh Ghodichor: Review on black hole attack detection in wireless MANET, IJERCSE, VOl-4, Issue-3, March 2017, pp 305-309

[9] Ola H. Younis, Salah E. Essa, Ayman El-Sayed: Defense Mechanisms in Mobile Ad-hoc Networks, Communications on Applied Electronics (CAE) – ISSN: 2394-4714, Foundation of Computer Science FCS, New York, USA Volume 7 – No.2, May 2017, PP 19-28

[10] Gautam Borkar, A.R. Mahajan: A review on propagation of secure data, prevention of attack and routing in mobile ad-hoc networks (MANET), International Journal of Communication Networks and Distributed Systems, 2020 Vol.24 No.1, pp.23 – 57

[11] Srivas Aluvaia, K. Raja Sekhar, Deepika Vodnala: A Novel technique for node authentication in mobile ad hoc networks, Perspectives in Science published by Elsevier vol-8, 2016, PP 680-682

[12] Pushpraj Niranjan, Prashant Srivastava, Raj Kumar Soni, Ram Pratap: Detection of worm-hole attack using Hop-count time delay analysis, IJSRP,vol2, issue4, 2012

[13] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma: A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks, JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617, PP 41-48

[14] Kirti Gupta, Dr. Pardeep Kumar Mittal: An Overview of Security in MANET, Gupta et al., International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-6) PP- 151-156

[15] Anju Markose, Asst. Prof. Vidhya P.M: Survey on Different Watchdog Systems to Deal with Selfish Nodes In MANETs, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 06-13

[16] Khaled Mohammed Saifuddin, Abu Jobayer Bin Ali, Abu Shakil Ahmed, Sk. Shariful Alam, and Abu Saleh Ahmad: Watchdog and pathrater based Intrusion Detection System for MANET, 2018 IEEE, pp 168-173

[17] Medi Sandhya Rani, Rekha Redamalla, K.V.N. Sunitha: Secure Group Key Exchange and Encryption Mechanism in MANETs, Chapter · January 2019, DOI: 10.1007/978-981-10-8201-6_43, pp 383-390

[18] M. El-Bashary, A. Abdelhafez, W. Anis: A Comparative Study of Group Key Management in MANET, M. El-Bashary et al. Int. Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 5, Issue 8, (Part - 4) August 2015, pp.85-94

[19] C. Perkins: Ad hoc On-Demand Distance Vector (AODV) Routing, The Internet Society (2003), RFC 3561

[20] Leighton Johnson: In Security Controls Evaluation, Testing, and Assessment Handbook (Second Edition), 2020 “Security component fundamentals for assessment” Encrypting Private Data-Employing Symmetric Cryptography, ScienceDirect is Elsevier’s leading information solution for researchers.