Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, October 2021: 20-48

Research Article

MANET Routing Attacks and Their Countermeasures: A Survey

Niranjan Panda [1], Bichitrananda Patra [2], Sarbeswara Hota [3]

Abstract

Mobile Ad-hoc Network (MANET) is sometimes described as an autonomous system designed through the coordination of a collection of mobile nodes that communicate with each other via wireless connections. Nodes in the network behave as end-systems as well as packet forwarding routers. Every node can move freely, change locations and configure itself to form a network. MANET poses challenges such as open peer-to-peer network infrastructure, shared wireless media, severe resource constraints and highly dynamic topology of network. Special / proper routing protocols are required to cope with the challenges. Choosing the algorithms had to understand the characteristics of the network, such as node density, size and mobility. The primary concern of routing protocols in MANET is to; establish an optimal and efficient route between the communicating parties. Any routing phase attack can disrupt communication and paralyze the entire network. Providing security for a protected communication between nodes in routing has thus become a prime concern. MANET's dependability and security aspects, such as jamming and eavesdropping, should be taken care for the users to perform secured peer-to - peer communication over a wireless multi-hop channel. A user must be provided with security services such as authentication, integrity, non-repudiation, confidentiality, key and trust management and access control, depending on the context of the application. In this paper we have tried to present the entire thing; starting from the basic concept of MANET, its architecture, routing protocols, attacks

[1] Department of Computer Science and Engineering, Siksha O Anusandhan (Deemed to be) University, Bhubaneswar, Odisha, niranjanpanda@soa.ac.in

[2] Department of Computer Science and Engineering, Siksha O Anusandhan (Deemed to be) University, Bhubaneswar, Odisha, bichitranandapatra @soa.ac.in

[3] Department of Computer Science and Engineering, Siksha O Anusandhan (Deemed to be) University, Bhubaneswar, Odisha, sarbeswarahota@soa.ac.in

during routing, security attributes and the proposed countermeasures at a single place. This paper will facilitate the researchers to understand the security challenges in MANET and motivate them to design a multi-fence security solution to achieve both bound protection and desirable network performance, considering all three security components detection, reaction and prevention.

Keywords: *MANET, vulnerabilities, routing protocols, multi-fence security solution*

Introduction

Mobile Ad-hoc Network (MANET) is gaining significance as one of the most novel and demanding aspects of wireless communication owing to the immense demand for wireless sensor network (WSN, disaster response), military application, collaborative and distributed computing, Medicare and enterprise solutions.

MANET is referred to as a group of autonomous mobile wireless nodes with self-organizing abilities gathered in an random and temporary network topology, linked via wireless channels. It's a decentralized systems with self-configuration and self-maintenance capabilities in which nodes in the network are in mobility, hence network topology may change rapidly and unpredictably over time. Each node behaves as both a router to forward packets and a host during communication with the neighbor node present in its transmission range. The nodes in themselves perform routing functionality incorporated in the mobile nodes and network actions including topology discovery and messages delivery in MANETs. To communicate with non-neighbor node peer-to-peer communication over multihop channels will be imparted in MANETs and the on-hop connectivity is ensured via datalink layer protocols with an expansion to multiple number of hops via network layer routing and data forwarding protocols. As the communication carried out over wireless links, the links have less bandwidth in comparison to wired network. Wireless connections can also deal with radio transmission effects such as noise, fading, and interference.

Due to its unique characteristics namely absence of infrastructure, shared channel for broadcasts, unguarded wireless domain, deficiency of central point of control, highly dynamic topology, and constrained resources, MANET is available to both genuine users and malicious attackers making the network vulnerable, in absence of traffic monitoring or access control. Hence security issues in MANETs depend on implicit trust relationship for routing packets between the participating nodes. The routing security service provisions in MANET depends on the supported application characteristics and the networked environment that may differ considerably but ultimately prevent attackers from disrupting the usual serviceability of the mobile network, maintaining the general security objectives such as authentication, availability, confidentiality, non-repudiation and integrity and addressing the fields like location confidentiality, cooperation fairness and absence of traffic diversion. MANETs distinctive characteristics imposes a number of non-trivial challenges to the security design.

In our study we have discussed the characteristics of MANET which makes it vulnerable to attacks during Section 2. In Section 3 MANET routing protocols are classified and Section 4 describes the routing attributes for the MANET routing and the attacks that can often carried out on MANET routing protocols. Section 5 explains the MANET security attributes and in Section 6 discussed the solutions provided by different authors to different attacks. Finally in Section 7 we have concluded our work.

MANET Vulnerabilities

MANETs are more impervious than the traditional wired network due to their characteristics. In this section, we discuss those features which make MANET more challenging for designing routing protocols and vulnerable to attacks.

2.1. Unreliability of Wireless Link

Wireless links have a substandard protection against noise, fading and signal inferences and thus the control message related to routing can be tempered. In contrast with wired networks, even the wireless links have less bandwidth. This makes the wireless links inconsistent and unreliable during communication between participating mobile nodes [1].

2.2. Dynamic Topologies

In MANETs, nodes are free to move in arbitrary directions and together they form a typical multi-hop network topology that changes at unpredictable times randomly and rapidly. As MANET possesses a frequently changing topology, each set of adjacent nodes must have to assimilate in the routing concern for prevention of those kinds of possible attacks that attempt to explore the vulnerabilities in a statistically designed routing protocol [1]. Here, due to the mixing of a number of Ad-hoc networks, possibility of duplication of IP addresses arises making the impersonation attack to occur.

2.3. Implicit Trust Relationship Between Neighbours

Real Ad-hoc routing protocols presume all the participating nodes in the network are honest. This feature directly empowers a malicious node to operate and attempt to paralyze the entire network, simply by supplying incorrect information and spreading it over the network [2].

2.4. Lack of Secure Boundaries

In comparison to conventional wired networks, the MANET is more vulnerable which means self-evident. Traditional wired network possesses a clear line of defense, whereas in the MANET, there exists no such clear secure boundary. In MANETs, each node is allowed to participate, quit and move within the network with full freedom. Lack of secure boundaries makes the MANET vulnerable towards the attacks. Hence, in MANET, any node can be attacked by other nodes present in its radio range at any moment of time and also being an

attacker, it may attack to another node(s) within its radio range. Various link attacks are there which may lead the situation to worse jeopardizing the MANET and making the network nodes difficult to withstand. Basically, the link attacks can be mainly classified as active interfering, message contamination, data tampering, message replay, denial of service, passive eavesdropping and leakage of secret information [3].

2.5. Threats from Insider Compromised Nodes

In a MANET, mobile nodes are independent units and they are free to participate in various activities or quit the network. Making some effective strategies for prevention of the viable malicious behavior from all the neighboring nodes, the node communicating with others becomes so difficult due to the behavioral diversity of the nodes. Whenever a large scale Ad-hoc network is considered, it becomes so difficult to trace the malicious behavior carried out by the compromised nodes as they change their attack targets frequently because of their mobility aspect. Hence, risk in the network from insider compromised nodes is much higher than the outsider nodes. Also, attacks by compromised nodes are difficult to detect as these nodes are considered as legitimate nodes before they are compromised.

2.6. Unavailable Centralized Management Facility

Ad-hoc network contains no centralized component of management mechanism like a name server. Owing to scarcity of centralized management facility, each node is allowed to take its own decision and hence, problems like transmission impairments, detection of attacks, packet dropping, path breakages and breakage of the co-operative algorithms occurs.

2.7. Restricted Power Supply

Nodes in a MANET are battery powered and for which energy must be conserved. So during system design, special care must be taken about optimization of energy and conservation of it. Taking the advantage of restricted power supply, an adversary node may flood additional packets to make target node busy in routing the additional packets or may persuade the target node for doing some lengthy computations. In both the cases, the ultimate aim of the adversary node is to drain the target node’s battery power, which leads it to a situation when it will be out of power and fails to provide service to genuine requests. This situation creates a denial-of-service attack [16].

2.8. Scalability

MANET suffers from the problem of scalability [3]. Traditional wired network generally comes with a predefined scale and the scale cannot change a lot during network operations. But in a MANET, the scale of the network alters frequently as the nodes are mobile in nature and we can’t predict the amount of nodes existing in the network in future. Hence, routing

protocols and services like key management must have to be designed in a way that they can be compatible with the MANET with a scale changing in time.

Routing in MANET

Routing is the mechanism required by each and every device within a communication network to communicate with the others. In other words, we may say that the routing algorithm consists of a group of instructions for transmitting data over an appropriate path between two devices in a network. In MANETs, a routing protocol makes use of routing algorithms to establish an optimal route in between the source node and the destination node for efficient data transmission [17]. Also, the route maintenance and repair during a link failure is the responsibility of the routing protocol.

3.1. MANET Routing Protocols

MANET routing protocols are categorized into different classes [4] based upon their characteristics of establishing the route and maintaining them during communication, as represented in Fig 1.

3.1.1. Reactive Routing Protocol

The reactive routing protocol uses an on-demand approach for establishing a route to the destination, after getting a request from the source [5]. Routing process includes two phases such as route discovery and route maintenance. A route discovery process is initiated and route requests (RREQs) are broadcast to its neighbouring nodes by the source node when it needs to send data in turn, the neighbour nodes rebroadcast the RREQ message until it reaches the destination [6]. The RREQ message holds a hop count field to determine the shortest path so as to approach to the destination, a source sequence number field to prevent loops and a destination sequence number field to obtain the freshness of the route during route discovery. The destination node receives the RREQ sent from the source and afterwards it transmits route reply (RREP) across the shortest path to the source. In the process of route maintenance, HELLO messages are used to observe the link status of the next hops during active routes and when a loss of link occurs, it is immediately notified by a route error (RERR) message.

Reactive routing protocols are more efficient at signalling, power consumption and also reduce the routing load by eliminating the use of routing tables and its updates during topology changes within the network. On the other hand these routing protocols suffer from a significant delay before packet transmission along with a notable amount of control traffic transmission. These sorts of routing protocol are most suited for networks where nodes are highly mobile or transmit data infrequently.

Ad-hoc On-demand Distance Vector (AODV), Cluster Based Routing Protocol (CBRP), Location Aided Routing (LAR), Power Aware Routing (PAR), Signal Stability Routing (SSR), Temporarily Ordered Routing Algorithm (TORA), Associativity Based Routing (ABR) Dynamic Source Routing (DSR), Dynamic MANET On Demand (DYMO) are examples of some reactive routing protocols.

3.1.2. Proactive Routing Protocol

Proactive routing protocols are essentially table-driven by design, and each node maintains the route details for the entire network. Any modification within the network topology is expressed by the periodic exchange of topology information between nodes within the routing table provided by each node [6]. HELLO messages are used for building the routing information at each node with the exchange of connectivity information and Topology Control (TC) messages that are used for maintaining the neighbour connectivity information [7].

Proactive routing protocols can establish quick routes with a smaller delay, but consume larger resources in terms of bandwidth, memory, power, etc. Also high mobility of nodes results in many short lived routes and leads to traffic overhead. This type of protocols is convenient for networks with low node mobility and frequent transmission of data from nodes.

Optimized Link State Routing (OLSR), Topology Broadcast based on Reverse Path Forwarding (TBRPF), Destination Sequence Distance Vector (DSDV), Wireless Routing Protocol (WRP), Cluster head Gateway Switch Routing (CGSR), Global State Routing (GSR), Fisheye State Routing (FSR), Hierarchical State Routing (HSR), Zone based Hierarchical Link State Routing (ZHLS), and Source Tree Adaptive Routing (STAR), Landmark Routing Protocol (LANMAR) are examples of some proactive routing protocols.

3.1.3. Hybrid Routing Protocol

Reactive and proactive routing protocols show optimum performance in different scenarios. A mixture of these two types of protocols, referred to as the hybrid routing protocol[8], proposes the use of proactive routing within certain areas and reactive routing within the remaining part of the network. The entire network is subdivided into small areas called zones[4] and the use of proactive routing within each zone reduces the overhead control and delays with the details available in the routing table. Due to its flexibility with bandwidth in continuously evolving network, reactive routing is used for routing packets across various zones.

Core Extraction Distributed Ad-hoc Routing protocol (CEDAR), Zone Routing Protocol (ZRP), Zone based Hierarchical Link State Routing protocol (ZHLS) are some examples of hybrid routing protocols.

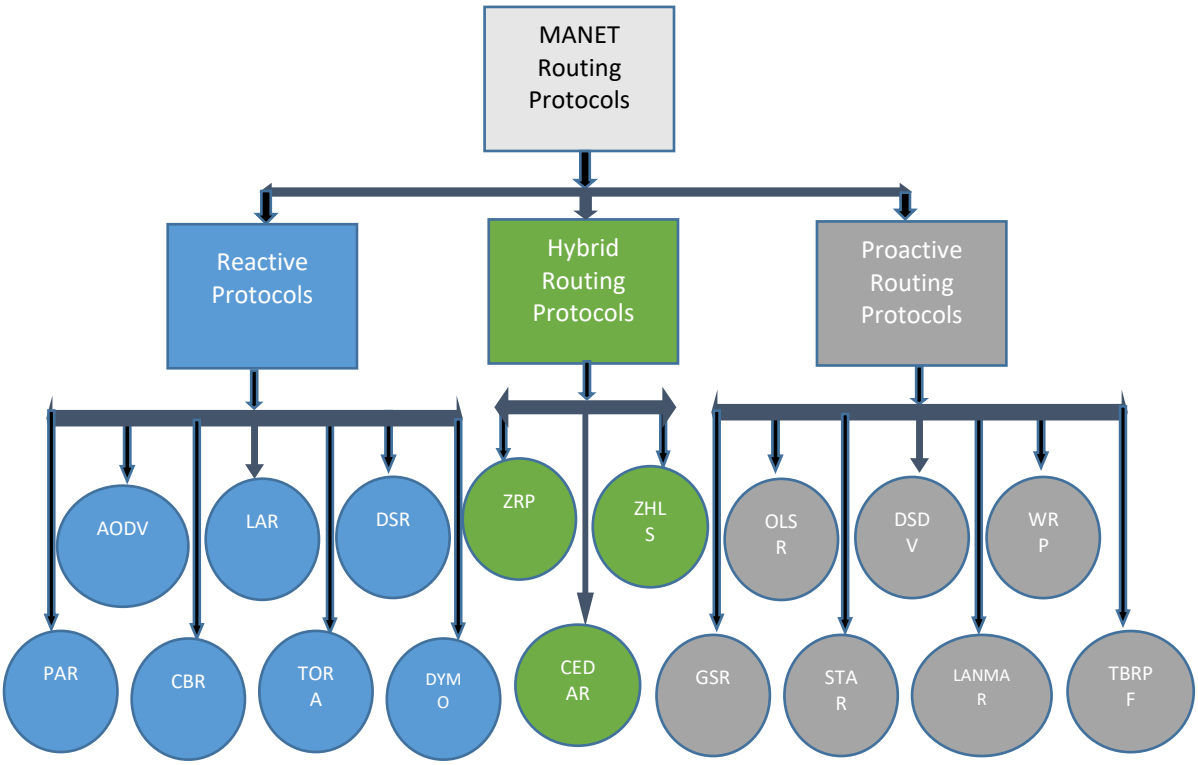

Fig 1. MANET Routing Protocol Classification

3.2. Routing Protocol Attributes

MANET is more vulnerable than the conventional wired network because of its characteristics, which are to be addressed here and taken care of during the development of MANET routing protocols.

3.2.1. Distributed Nature of Implementation

Ad-hoc networks are wireless in nature with autonomous and self-configuring capabilities. So routing protocols designed for MANET must not be dependent on any centralized controlling authority, and should be distributed in nature.

3.2.2. Efficient Utilization of Bandwidth

In MANETs, bandwidth is limited, which puts a limitation over its consumption by control traffic. Hence, design of routing protocols must take care of reduced control overhead and handling excessive control traffic.

3.2.3. Efficient Utilization of Battery Capacity

Unlike wired networks, nodes in MANET suffer from low battery power which impacts its performance. Hence, during communication in MANET, nodes must accommodate sleep periods when they are idle from transmitting and receiving signals for increasing the lifetime of hosts in the network.

3.2.4. Freedom from Loops

In MANET routing algorithms, looping of packets can cause overhead in terms of bandwidth and power consumption. Hence, loops must be avoided in routing tables for a better performance during communication and can be achieved using TTL (Time to Live) values.

3.2.5. Unidirectional Link Support

Bidirectional link combining unidirectional links must be constructed efficiently in MANET as routing protocols designed to use the unidirectional links for a better result considering the factors like radio capabilities and signal interference.

3.2.6. Fast Route convergence

Topology of MANET changes dynamically leading to the need of convergence of a new and stable route as soon as possible after a link failure. Hence, routing protocols must be efficient to provide fast and accurate route information in wireless Ad-hoc environment.

3.2.7. Optimization of Metrics

Routing in MANET also suffers from different metrics other than bandwidth and battery power, depending upon the type of protocols. Metrics like end-to-end delay, end-to-end throughput, number of hops, congestion, adaptability to change topology, association stability influence routing protocol operations and should be considered during routing protocol design.

Classification of Attacks in MANET

This section basically classifies attacks into different types considering different points of view about an attack.

4.1. Routing Attacks based on Action of Attackers

Attacks in MANETs are basically classified into three types as passive attack, active attack and collaborative attack depending upon the actions of an attacker to be performed during an attack and the attack being performed by the attacker independently or collaboratively with other attackers.

4.1.1. Passive Attack

In Passive Attack, an access control aims to stop the illegitimate use of the available network resources and the services offered. The attacker just focuses on the channel and packets carrying secret information like IP addresses, network topology information etc. without any

disruption in the operation of routing protocols. Unauthorized listening by routing packets violates the confidentiality attribute of wireless communication. Passive attacks are cooperative, non-troublesome, but information striving in nature which further provide a platform further for active attacks by the attackers to happen. Passive attacks are regularly extremely hard to identify.

4.1.2. Active Attack

In active attack, an attacker replicates, modifies or deletes the packet's contents or injects packets to invalid destination inside the network in an aim of disrupting the normal response of the protocol. This type of attack violates availability, integrity, non-repudiation and authentication attributes of the wireless communication. Active attacks can be detected on a network more easily in comparisons with other attacks which makes it less frequently used by the attackers.

4.1.3. Collaborative Attack

In Collaborative Attack, a group of attackers work together to disturb a network directly or indirectly. In indirect collaborative attack, non-existent attacker nodes fake legitimate nodes for directing packets to particular malicious nodes. The routing protocols affected by blocking the routing information to propagate to a node and packet forwarding as well as delivery mechanism are affected by disturbing the packet delivery against a predetermined path in this attack. Basically Sybil and routing table overflow attack falls into this category of attack. In direct collaborative attack, the attacker nodes join or exist in a network before. Basically, attacks like blackhole and wormhole falls into this category.

4.2. Routing Attacks based on Operational Ideologies

Basically, considering the working principles and effects of attacks, they can be classified into different categories as explained below.

4.2.1. Routing Table Overflow Attack

In this attack, the entire network is crowded with excessive route advertisement to non-existing nodes. This prevents the creation of new routes and overwhelms the protocol implementation. Proactive routing protocols are more vulnerable to this type of attack as routes are created and maintained for all possible destinations in this type of protocols.

4.2.2. Flooding Attack

In this flooding attack attackers flood the network with bogus messages to fake nodes or arbitrary destinations with an aim of wasting the resources like bandwidth, computational power, memory, battery power which may further prevent the network from functioning properly. In reactive routing protocols, RREQ messages are flooded and in proactive routing

protocols network is flooded with TC messages. In the proactive routing protocol, TC message's route is not controlled making it more vulnerable to this type of attacks in comparison to reactive routing protocols.

4.2.3. Sleep Deprivation

Sleep deprivation attack is considered to be a distributed denial of service (DDoS) attack based on the energy constrained operations in MANET. An attacker node interacts with the legitimate nodes being legitimate, but the interaction is meant for disturbing those nodes to go into sleep mode keeping them busy in routing decisions. In reactive routing protocols, an attacker takes the benefit from the vulnerabilities of the route discovery process and keeps the nodes busy by flooding the network with malicious RREQ messages. Malicious RREQ flooding is further classified into two categories. In the first case, the RREQ incorporates a destination IP address of a fictitious node where no node within the network contains a valid route towards the destination, but still they forward the RREQ packet. In the second case, without waiting for the ring traversal time, the attacker node continuously re-sends the RREQ packet for the identical destination node with higher TTL values. In proactive routing protocols, the uncontrolled transmission rate of the TC messages leads to this type of attacks.

4.2.4. False Removal of Working Route

In this type of attack, malicious nodes manipulate the RREQ message and intimate the upstream nodes with a false state of links which leads the source node to start a current route discovery operation with a higher cost in terms of time delay and resource consumption. This attack may occur when an attacker node initiates the RRER message to the up-link nodes being the part of route falsely intimating a loss of link or by masquerading and sending a spoofed message while not belonging to the route.

4.2.5. Impersonation Attack

In impersonation attack, attacker nodes impersonate legitimate nodes or we can say that the attacker nodes steal the identity of legitimate nodes to participate in a network and imperceptibly convey false routing information being masked as some legitimate node. Attackers stays in the middle of communication between two communicating nodes, mask their IP addresses and launches an impersonation attack without their awareness of someone being present in between them.

4.2.6. Node Isolation Attack

In proactive or table driven routing protocol like OLSR, attackers block route information about a particular node or a class of nodes to be disseminate in the entire network. By virtue of this, other nodes of the network fail to receive the link information about the existence of

these nodes and can't build a route to these nodes. Hence, the targeted nodes behave as isolated from the remaining nodes in the network.

4.2.7. Routing Table Poisoning

In this attack, a malicious node makes false entries to the routing tables maintained by different routing protocols by generating and sending fictitious traffic or mutating authenticated messages from different nodes. Also, injecting RREQ messages with a higher sequence number by an attacker deletes other genuine routes with lower sequence numbers resulting in a corrupted or poisoned routing table. This type of attack leads to the selection of non-ideal routes, creating loops in routing, bottleneck and even isolating certain parts out of the whole network.

4.2.8. Location Disclosure Attack

In this type of attack, the security prerequisites of a MANET are jeopardized using the techniques like traffic analysis or sampler probing and traffic monitoring approaches. The attacker discovers the position of the node and the layout information of the entire communication network.

4.2.9. Blackhole Attack

Attacker nodes in blackhole attack use the flaw in the process of route discovery of reactive protocols, and insert false route to destination node. When an RRER message is sent, an intermediate attacker node transmits an RREP message with a higher destination sequence number compared to the sent RREQ message stating a path to the destination. If an intruder prefers the idea of rushing along with high-power transmission creating this attack, finding a path that does not pass through the assailant node is utterly impossible. If the node is selected as an intermediate node or is part of the network routes begins to misuse or discard the routed traffic by forming a blackhole. When the attacker is part of several paths, this attack could be serious.

4.2.10. Grayhole Attack

Grayhole attack is an unusual instance of blackhole attack in which an intruder node is part of a network route as in blackhole attack, but does not completely drop the routed data packets. Attacker nodes can initially act as legitimate nodes in order to gain trust, but then drops packets selectively with some probability from some particular nodes or in some other similar pattern. For this sort of attack, it is very difficult to detect attacker nodes because these nodes drop packets sent through them for certain period, while they would act usually as legitimate nodes for the remaining time.

4.2.11. Wormhole Attack

Wormhole attack involves co-operation between two attacking nodes and is also known as a tunnelling attack. One attacker captures the routing packets at a specific location within the network and tunnels those packets at a distant location (may be several hops away) to the second attacker bypassing the intermediate nodes. The second attacker replays the received packets again into the network. The tunnel shares a private fast transmission link between the attackers using either In-Band channels or Out-Band channels. In-Band channels employ encapsulation to build up a secret overlay tunnel over the current medium, whereas Out-Band channel use external communication medium like long range remote transmission or private rapid network to set up an immediate connection between the two conspiring nodes. The tunnel so made gives a feeling that the attacker nodes are next to each other or one hop away in view of hop count, making the wormhole invisible. Therefore a wormhole delivers RREQ messages faster than the legitimate paths, making the nodes to only find a route through it. Further, the colluding attackers may sniff or drop the data packets prompting DoS attack, distorting the topology and making the route under the dominance of the wormhole link. Wormhole attack is possible whenever all communications impart authenticity and confidentiality. Hence, wormhole attack is threatening for table-driven as well as the on-demand routing protocols.

4.2.12. Rushing Attack

In rushing attack, a spiteful node broadcasts a rushed RREQ message to reach each neighbour of the target before the RREQ messages of the legitimate nodes causing the legitimate RREQ messages to be discarded. So the initiator node during route discovery fails to discover any route with length more than two hops that does excludes a route through the attacker node. In reactive routing protocols, the RREQ messages are delayed due to an exponential back-off and in-frame spacing on the MAC layer mandated by IEEE 802.11 and the delay in preventing collisions between receiving and retransmitting an RREQ message which makes it easy for an attacker to attack. An attacker to make a rushing attack may use the techniques of broadcasting RREQ messages at a higher power level for a long range transmission skipping some intermediate hops to reach the destination first. Also, an attacker may forge and redirect rushed RREQ message with a larger source sequence number assigned. A network layer rushing attack requires a single insider node and secure routing protocols like Secure Ad-hoc On demand Distance Vector (SAODV), Authenticated Routing for Ad-hoc Networks (ARAN), Secure Dynamic Source Routing (SDSR), A Secure On-Demand Routing Protocol for Ad-hoc Networks (ARIADNE) are vulnerable to this type of attack.

4.2.13. Sybil Attack

In MANET, every node needs a unique identity to be a part of the routing. An attacker node manages multiple identities in sybil attack and generates a number of virtual nodes with new identities using fresh randomized creation or impersonating or spoofing some other valid node identity to generate confusion in the routing process or disrupt the entire network. Sybil attack targets MANET 's property of not having a centralized management system or authority for identity verification. Both table driven and on-demand routing protocols are susceptible to Sybil attacks. In table-driven routing protocols, a spoofed identity malicious node misdirects information to the spiteful node, while the routing mechanism in reactive nodes is interrupted by creating counterfeit identities that lead to DoS attack.

4.2.14. Blackmail

Due to insufficient authenticity, any node can be able to corrupt the information of the other legitimate nodes. Using this advantage, an attacker may fabricate the reporting message used by some routing protocol that propagates message to blacklist some malicious nodes found, blacklists legitimate nodes to isolate them from other nodes.

4.2.15. Snare Attack

Snare attacks relate to specific military uses. A physically compromised node becomes very important for an attacker as it can be used to intercept all the transmissions in the network passing through it. An attacker can locate a Vehicle Identification Number (VIN) using trace and analysis of some routes which may further lead to a decapitation strike to win the battle.

4.2.16. Invisible Node Attack

Invisible node attack defined in has been claimed to be an unsolvable attack. A node that takes part in the routing process without disclosing its identity, in any routing protocol that relies upon recognizable proof for any functionality, termed as an invisible node. In presence of such type of nodes the activity and effect of routing protocol is termed as Invisible Node Attack (INA).

Security Attributes

Security can be described in MANET by analyzing some specific attributes. These attributes are described in greater detail below.

5.1. Availability

The term Availability means the ability to provide services in any situation without considering its security state. DoS attack mostly affects this attribute.

5.2. Integrity

The integrity of a message guarantees its identity during transmission. Integrity can be affected accidentally in between the transmission of messages or maliciously by an adversary

node. In accidental altering, a message may be lost or get modified due to hardware failures and transmission errors during communication. On the other hand, an adversary node with a malicious aim drop, fabricates or replays a message in malicious altering.

5.3. Non-repudiation

Non-repudiation keeps a sender node trustworthy. If a node sends a message it can no longer refuse the fact that it has sent the message. Signature based schemes can be used for the message to maintain non-repudiation. Using public key cryptosystem, a particular sender node sends a message after signing it using the private key. Every other node confirms the signed message received by using its public key and, that particular node cannot deny about the message.

5.4. Confidentiality

Confidentiality ensures that all information is available only to their designated entities and can not be revealed to unauthorized entities.

5.5. Authenticity

Authenticity assures the participation of genuine communication participants and not impersonators. In order to avoid unauthorized access to resources and sensitive information, communication participants must prove their identity.

5.6. Authorization

Authorization is a process of issuing credentials to entities about the privileges and permissions granted to them and cannot be forged by the certificate authority.

5.7. Access Control

Access control aims to forestall illegitimate usage of network resources and services. It governs the way the users can have access to data. The access control mechanism is associated with authentication attributes. Access control involves the mechanism for forming a group of nodes, communicating a newly logged node with other nodes present earlier on the network etc.

5.8. Anonymity

Anonymity signifies that the identity information of the owner node should be kept private and cannot be interrupted by any other system software nor by node itself for protecting the privacy of the node from discretionary revelation to some other entities.

Security Schemes

A variety of security mechanisms have been invented to securing a MANET. Broadly we can classify them into two approaches: proactive and reactive.

Proactive mechanism is also known as preventive mechanism. In proactive approach we attempt to provide first line of defence typically through various cryptographic techniques such as hash functions, threshold cryptography, digital signature, asymmetric and symmetric key cryptography etc. The reactive mechanism, on the other hand, seeks to identify posterior threats providing a second line of defence and react accordingly. Both the approaches has their own merits depending upon situations and fits suitably for addressing different issues in MANET routing. For example, proactive approaches are used in most of the secure routing protocols for securing the exchange of routing messages between mobile nodes, on the other hand to protect packet forwarding operations reactive approaches are mostly used.

6.1. Defence Method Against Flooding Attacks

Yi et al. [11] presented an approach for prevention of flooding attack in AODV, in which neighbours RREQ rate is monitored by each node and if exceeds the threshold value defined before, then all further RREQs dropped declaring the neighbour node as blacklisted. This approach fails when attackers flood below the threshold value defined before or impersonate legitimate nodes id large number of RREQs.

Guo et al. [12] presented a technique for detection of blackhole attack which uses the non-parameter CUSUM algorithm and termed as flow based detection mechanism. For flooding attacks with randomly generated source and destination addresses CUSUM algorithm used for detection of threshold for attack in DSR protocol.

V. Boppana et al. in [13] suggested an Adaptive technique to prevent flooding attack with varying rates based on statistical analysis in which each node maintains a table to keep the track of RREQ rates for each of its neighbouring nodes. A neighbour node Id is blacklisted when its RREQ rate becomes more than the threshold value determined on the basis of statistical analysis of RREQ Floods.

H.Nair and S.Nair in [14] proposed a flooding attack defence mechanism based on a packet filtering firewall concept. A firewall is used to act as a fence between the internal and external network and to monitor the packets incoming and outgoing. This suggested model prevents unauthorized access by malicious nodes, but fails when the traffic can’t be denied.

N.Raj et al. in [15] suggested a solution to prevent SYN flooding attack based on traffic analysis, prediction and pre-processing mechanism. A node monitors the traffic collecting information about the nodes sending packets. When the traffic increases abnormally the malicious node is predicted and blacklisted based on the collected information. In this scheme we have to monitor the traffic continuously in small interval of time.

6.2. Defence Against Blackhole Attacks

Saetang et al. [16] suggested a credit based technique for elimination of blackhole attack known as Credit based on Ad hoc On-demand Distance Vector (CAODV) routing protocol. The next hop availability is decided based on credit values. During route discovery a node that exists within the route table when sends a packet, a credit of the next hop is decreased. Upon receiving a data packet destination node replies with a Credit Acknowledgement (CACK) to the source. Each intermediate node is responsible for increasing the credit value of the trusted next hop. Whereas on those situations where data pacts fails to reach destination an intermediate nodes fail to receive CACK the credit value falls to zero, blacklisting the next hop.

Sen et al. [17] proposed a low cost solution for detection of cooperative blackhole attack in standard AODV protocol which reacts to malicious activities of the internal nodes by detecting them. The major advantage of this proposal is, it doesn't use cryptographic techniques whereas suffers from a relatively high detection rate with modest network traffic hidden overhead and computation overhead.

Wei et al. [18] proposed a solution based upon two related algorithms: key management algorithm based on gossip protocol and detection algorithm based on aggregate signatures. Every node associated in a session creates an evidence that it has accepted the message; whenever any misbehaviour is detected by the source node, intermediate nodes are checked using a check-up algorithm and depending upon the facts returned by the check-up algorithm, the malicious node are detected by diagnosis algorithm. This protocol is subject to high traffic and computation costs for the detection of hole attacks.

Gonzalez et al. [19] proposed a threshold based approach to distinguishing between well-behaved and misbehaved nodes for detection of grayhole and blackhole attack which use the principle of flow conservation and accusation of misbehaving nodes. The downside with the scheme is that nodes can drop packets until being charged and, during the preliminary process, might get disconnected from the network.

Pu et al. in [20] proposed an exploration-based active detection system (EBAD), to effectively prevent routing misconduct in MANETs. In this system, a source node broadcasts a packet of RREQ with a fictitious destination node to attract possible malicious nodes to respond to a false RREP packet. Whenever a false RREP packet is received by the source node, or the received RREP packet cannot be decrypted by an intermediate node, then a routing misconduct may

A routing algorithm based on the sending of fake packets is proposed by Delkesh and Jamali in the paper [21] to increase the efficiency for detection and removal of malicious nodes. The

malicious network nodes are detected by transmitting forged RREQ and RREP routing packets that includes the address of a nonexistent destination node. Then, by sending an RREP request, they are deleted from node routing tables. This suggested approach has been able to increase network traffic load, find a short and safe path, detect the misbehaving nodes and optimize the network parameters.

Veeraiah & Krishna [22] suggested a trust-aware scheme based on fuzzy clustering and Naive Bayes method for detecting MANET intrusion. The fuzzy definition of clustering specifies the cluster-head for the clusters to shape. In addition to direct trust, indirect trust, and the recent trust, the proposed BDE-based confidence factors keep the node information and the Fuzzy Naive Bayes approach used to evaluate node intrusion using the node trust table.

6.3. Defence Against Grayhole Attacks

Jhaveri et al.[23] suggested a grayhole attack prevention strategy focused on the estimation of a peak value in AODV routing protocol. A peak value is calculated by each node and after receiving a RREP packet, the destination sequence number is compared with the peak value calculated. Finding the destination sequence number is higher than the calculated peak value of the node, the RREP received is discarded otherwise the RREP is processed. Hence RREPs from the malicious nodes are already dropped by the intermediate nodes in the path by reaching the source avoiding the grayhole attack.

Nadav et al. in [24] suggested an approach for minimization of grayhole attack in MANETs. The propose scheme assumes that each attacker node gains its knowledge by routine routing information and no collaborative attack to be performed. Evaluation of the scheme is made using different attack models depending on attacker capabilities.

In [25], Panda and Pattanayak analysed the effect of grayhole and blackhole attack on various routing protocols like AODV and DSR and later in [26] presented the idea of an Intelligent Mobile Node that effectively detects grayhole, blackhole attacks and can take action against such attacks after detection. The suggested mechanism involves some extra costs to implement the Static Intelligent Nodes in the network, but minimizes the packet loss giving a raise to the throughput of the network.

6.4. Defence Against Wormhole Attacks

Hu et al.[27] put forward the concept of packet leashes to detect and avoid wormhole attacks. These packet leashes are classified into two categories such as temporal leashes and geographical leashes. Temporal leashes use the speed of light for computation of packet expiration time. Initially, the sender sends the packet along with its creation time and at the

receiver end current time and the expiration time of the packet is compared and the packet expiry time is computed, preventing the packets to travel further than a specific distance. Also TIK protocol proposed by the authors (which stands for TESLA with instant key disclosure, and is an extension of the TESL protocol) [28]. For authenticating the expiration time preventing its modification by the malicious nodes. In this scheme tightly synchronized clocks are maintained by each node.

Tran Van Phuong et al.[29] suggested an approach for detecting wormhole in MANET and presented a time-based mechanism using the Round Trip Time (RTT) value. The RTT is the time elapsed between sending the RREQ to a remote node and receiving the RREP when the route is established. Wormhole is identified when a route possesses substantially longer RTT value, as the time taken for a transmission between two fraudulent neighbours produced by wormhole is much more excessive in comparison to the time between two legitimate neighbours. No special hardware needed to implement this mechanism and an assumption has been made that the source and the destination nodes are reliable. This scheme fails to detect exposed attacks where fake neighbours are not created. The attackers may also fabricate the RREQ or RREP time stamp to evade the rule of detection.

Khalil et al. [30] proposed a mechanism based on local monitoring by nodes for detecting wormhole attack in static networks called LiteWorp. Each node monitors its first and second hop neighbours for all the incoming and outgoing traffic. The guard node monitors a legitimate link between two nodes being a common neighbour to them and a wormhole detected when a neighbouring node is found to behave maliciously. LiteWorp is a low cost solution for wormhole detection but finding a guard node for a particular link in sparse networks is not always possible.

A secure mechanism against wormhole attack in MANET proposed using Honeypot [31] based on dynamic learning about the environment and being self adapting to evade malicious nodes. Honeypot helps to discover and learn the activity of intruder nodes and notice, catch and misguide the intruder nodes during their attempt for an unauthorised access or system attack providing a measure to improve network security. More over Honeypots provide an advance knowledge about an attack before its occurrence along with the methodology, tools used and vulnerability to target by an attacker.

Qian et al. [32] proposed statistical analysis multi-path (SAM), an approach for detecting wormhole attack using multi-path routing. For one route discovery when all the routes are obtained, a statistical analysis is made and for each link appearing in those obtained routes relative frequency is calculated. Due to tunnelling, the path with wormhole nodes appears to

be smaller than normal paths making it attractive to route discovery. The attack is detected by finding the link with highest relative frequency as the wormhole link.

Yun et al. [33] suggested an approach called WODEM (Wormhole Defence Mechanism) against the wormhole attack with a few detector nodes having longer-lasting batteries and location-aware devices like GPS technology with a capability of transmitting data at different powers. Normal network nodes are only used for forwarding control packets from detector nodes.

Choi et al. [34] presented a method for the prevention of wormhole attack known as WAP (Wormhole Attack Prevention) which relies on the concept that every network node should monitor the activity of its neighbouring nodes by maintaining a neighbour table that contains sequence no. of RREQ, ID of neighbour node, RREQ sending and receiving time and the RREQ count. A wormhole prevention timer (WPT) is set by the source node and the delay per hop value must not exceed it. This method uses an end-to-end signature authentication of routing packets.

Biswas et al.[35] provided an enhanced version of the previous "WAP" approach by adding the ability of detecting a false positive alarm named s WADP (wormhole attack detection and prevention). WADP is integrated with node authentication in the modified AODV for providing a two way verification.

Chourasia and Singh [36] collected the values of hop count and delay per hop for divergent routes between source and destination and used those values to suggest a technique for wormhole attack detection in AODV routing protocol known as Modified AODV. It uses a twostep algorithm to compute delay and hop count information at destination in first step and the detection on the wormhole attack based on prior step knowledge in the second step.

6.5. Defence Against Rushing Attack

Hu et al. [37] analysed the way of launching a rushing attack in DSR. They suggested a set of generic mechanisms to prevent rushing attack; secure neighbour detection, secure route delegation and randomized route request forwarding. The mechanism secure neighbour detection is hinge on tight delay transmission timing to set a maximum transmission distance allowing each neighbour to verify that other node is within the communication range, preventing neighbour impersonation due to tunnelling and rebroadcasting packet. The nodes never forward RREQs from non-neighbour nodes. A node determines that its previous hop node is a neighbour and then only a route delegation message is signed letting it to forward the route request. Instead of the conventional duplicate suppression used in on-demand route

discovery, the route request to forward is randomly selected ensuring that the route request arrives earlier are only somewhat more probably to be forwarded.

Papadimitratos et al. [38] presented a Secure Message Transmission (SMT) protocol for protecting data forwarding operation. SMT is vulnerable to routing attacks like rushing attack and protocol like Secure Routing Protocol (SRP) is used to securing it. However the successfulness of SRP against the routing attacks was not evaluated by the author. Further Rawat et al. in examined on SRP the effect of rushing attack and put a conclusion that SRP can withstand the attack.

6.6. Defence Against Node Isolation Attack

Kannhavong et al.[39] stated that in the OLSR protocol, a mischievous node functions as a barrier to prevent, disrupt or isolate a particular node. The mischievous node prevents the legitimate node from receiving the data packets by withholding the TC messages. Also a node isolation attack detection technique is presented based on the monitoring of TC messages and HELLO messages generated by the MPR nodes.

Dhillon et al. [40] proposed an IDS (intrusion detection system) for OLSR protocol which identifies the TC link and message withholding attack, but this scheme fails when two colluding next hop attacker nodes work and the earliest one advertises a TC message whereas the subsequent one drops them.

6.7. Defence Against Sybil Attack

Douceur [41] proposed that elimination of sybil attacks in wireless networks is only possible through trusted certification. For which a Central Certification Authority is needed to be established for distributing certificates with digital signature to all the participating nodes. This approach is not suited for open MANETs. Further Sarosh et al. [42] classified the authentication techniques as; Central Certification Authority, Self Certification Authority and Distributed Certification Authority. Central Certification Authority protects sybil attack with the help of a trusted third party for issuing certificates to a participating node. Self Certification Authority fails to prevent sybil attack but it requires no additional resources. Distributed Certification Authority concentrates on generation and verification of cryptographic identities and vulnerable to sybil attack due to lack of verification of the credentials for a new node. Also an authentication mechanism with minimal with minimal support from the trusted third party is proposed based on the co-operative behaviour of the nodes for information interchange. This proposal provides an advancement for the earlier techniques where the problem of selecting a trusted was there.

Sohail et al.[43] presented a distributed framework to detect sybil attack based upon the principles of directional antennas for nodes to obtain their location. In this scheme hop by hop protocol layer information is used and a proof of traffic observation maintained in form of digitally signed packet digest by the sender for each packet sent by it. This scheme fails when colluding nodes fabricate location or time-stamp to make a sybil attack.

Piro et al. [44] proposed a solution in which node mobility is used for identifying sybil attack on MANETs. Multiple trusted nodes collaboratively or a single node alone may keep the track of the IP or MAC address of nodes to identify an attacker.

6.8. Defence Against Snare Attack

Lin et al. [45] proposed An Anonymous Secure Routing Protocol (ASRPAKE) based on authentication key exchange in wireless Ad-hoc network and installation of decoy nodes to prevent snare attack. ASRPAKE classified into different phases like; key pre-distribution, neighbourhood discovery, route discovery, route reverse and data forwarding. This approach provides end-to-end anonymity and security, along with integrates key exchange with authentication into routing algorithm. In this scheme only routing to the VIN is possible after complete verification of the authentication of the source node.

6.9. Defence Against Resource Depletion Attack

Gratuitous RREQ message: Gada et al. [46] proposed a solution to AODV and SAODV for the problem of RREQ flooding. Perkins et al. [47] proposed RFC 3561 based on a limit parameter over RREQ rate which provides a solution for limited problems and vulnerable to attack when a malicious insider node changes the limit value to congest the network.

Combating gratuitous data flows: Ramanujan et al. [48] proposed a routing algorithm (TIARA) based on Flow based Route Access Control (FRAC), multi-path routing, fast authentication, flow monitoring and network resource allocation for preventing intrusion attacks due to gratuitous data flow. FRAC used as a distributed firewall with light weight fast authentication.

6.10. Other Security Solutions

Many other security solutions are proposed to provide a secure routing in MANET and here we have considered some of them.

Marti et al. [49] proposed the concept of watchdog and path ratter for improving the performance of MANETs in presence of turbulent or misbehaving nodes. A misbehaving node may be overloaded, selfish, malicious, or broken in nature. Watchdog maintains a buffer to which those packets to be transmitted are copied and the behaviour of its adjacent node is monitored. Watchdog promiscuously snoops the packets are snooped indiscriminately by the

watchdog for a match in the observing node's buffer, and when a match occurs then they are discarded; otherwise the packets which are waiting more than a threshold time period with in the buffer marked as modified or dropped. The sender node for this packet initially considered to be suspicious and later on making greater number of violations marked to be malicious. Information about the malicious nodes collected by the watchdog is conveyed to the path ratter module for use in path rating evaluation. Path ratter works on each node to rate its neighbors based on the information passed by the watchdog with respect to their reliability.

Security-based on "self-healing community" is suggested by Kong et al.[50] which shows effectiveness towards the defence of ad-hoc routing protocols against adversary nodes. In community-based security, node redundancy explored on a per-community basis rather than per node basis at each forwarding stage. A self-healing community can be created or configured with compatibility to ad-hoc routing protocols. However, they may be reconfigured to accommodate the changes in the network based on node volatility, channel fluctuation, addressing and resolving non-cooperative nodes, etc. A chain of self-healing communities can be present in the common path, where each community comprises multiple peer service providers.A self-healing community functions well until a single cooperative node exists within the community. Self-healing community defends the attacks that use several cooperative network members and distinguished packet losses to deplete ad-hoc network resources by providing a countermeasure using the cooperative network members to tolerate the presence of non-cooperative members and stopping disruption attacks locally and immediately, which can't be answered by purely cryptographic solutions.

SMT (secure Message Transmission) protocol [38] combines end-to-end secure and robust mechanism, dispersion of transmitted data, simultaneous usage of multiple paths and adapting the dynamic changes in the network. SMT mainly supports quality of service (QoS) for real time traffic. In SMT source and destination nodes employ a secure communication in between them by authenticating each other. Then a set of diverse paths are found in between the source and destination node from the current network topology. Source disperses a message into N number of pieces and transmits them across the paths, so that destination can reconstruct the original dispersed message by combining successfully received pieces. Each dispersed piece assigned with a MAC or verifying its integrity, reply protection and authenticity of origin. Destination acknowledges each successfully received message piece by a feedback to the source. If enough pieces are successfully received at the destination, the message will be reconstructed, or else it will wait for the missing packet being retransmitted

by the source. Source re-encodes and re-allocates the undelivered messages over the path set for the transmission. The end nodes need to be successfully associated to each other, whereas none of them needs to be securely associated with any of the remaining nodes in the network. Therefore no cryptographic operations are needed at the intermediate nodes. Using feedback system, a piece that has been successfully obtained implies route to service while a loss suggests the path to be disrupted or compromised.

An Intrusion Detection System [51] (or IDS) generally detects unwanted manipulations to system. In IDS basically two types of models are implemented; anomaly detection and misuse detection. It works in three basic steps; to control the collection of data (monitor), decides the data collected indicates an intrusion or not (analyse), and manages the response action to the intrusion (response). Intrusion Detection may work in a distributive or cooperative environment for MANET. Each mobile node in a MANET has an individual IDS agent running independently to monitor local activities and identify possible intrusions. Various solutions are proposed to address intrusion detection in MANET.

MAC (message authentication codes) algorithms referred as keyed hash functions [52] as they use one way hash function and take a secret key as argument for producing a specified length output from a message with random length. For two nodes with a shared secret key K, a authentication tag T=MACk(P) is generated for message P using key K by the sender and(P,T) pair is sent to the receiver. Using the same key K and the authentication tag the message pair is verified on the receiver side, assuring authentication to the legitimate users only. CMAC is a derived version of CBC-MAC (Cipher-Block-Chaining) in which the plaintext or the input message is broken into N block encrypted iteratively and XORed with next block until the last block. The last block is XORed with two key dependent constants to yield a authentication tag. Here the message size must be known before the computation of the tag and for each message of different length additional encryption needed. PMAC1 (parallelizable MAC version 1) is a simplified version of PMAC, in which offsets are produced though finite field multiplications of an offset seed R. further variants of this are propose to be iPMAC which is supporting faster ad word oriented generation of offset. GMAC (galois MAC) is a variant of the GCM authenticated encryption which follows Carte-Wegman design [53] to reduce the amount of processing for its operation. GMAC are difficult to implement an main focused for powerful platforms.

In RSA like symmetric cryptographic schemes much more computations are needed for the signing and verifying operations of a signature. An attacker node floods victim node with a huge number of fraudulent signatures, exhausting victims computational resources used for

verification purpose. Along with that a certificate of revocation (CRL) must have to be kept with each node. Whereas digital signature scheme uses symmetric key cryptography and can be verified by a node knowing the public key of signer. Same number of public/private key pairs needed as the size of the network, which makes it scalable to a huge number of receivers. It provides more resilience against DOS attacks and the digital signature approach used by SAODV [54] protocol.

Conclusion

It is justified to say that MANETs throws a very composite and challenging problem towards research in aspect of its security. As no recognised infrastructure or centralised administration exists, attackers can access the network with ease. We addressed some common and dangerous vulnerabilities and security threats in the MANET, listed a number of network layer-related attacks and how security services can be accomplished for a safe routing across different security requirements. Also we can say that some attacks may lead to cause other attacks and should be given attention separately providing high degrees of security during routing in MANETs as they are inherently vulnerable to security attacks. Therefore secure routing mechanisms are absolutely necessary for Ad-Hoc Networks. Ad-Hoc Networks need very specialized security methods, as each network differs according to its construction and a single approach may not be fit for all of them. On a network the nodes can be any devices that are depending upon the type of node: and no assumptions on the node can be made.

Security in MANET is major research area for researcher today. Existing research works provides solutions to many attacks still many other unanticipated or collaborative attacks remain undiscovered till today. Hence researches still to continue for discovering many new threats as well as the solutions to them. More research is needed in the field of efficient key management technique, trust-based approaches in routing, security during routing, and securing data at different layers of communication.

References

ZaibaIshrat, “Security issues, challenges & solution in MANET”, IJCST, Vol. 2, Issue 4, Oct .-Dec. 2011.

Praveen Joshi ,” Security issues in routing protocols in MANETs at network layer”, Elsevier, Procedia Computer Science 3 (2011) 954 – 960.

Amitabh Mishra, Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

D. Kaur, N. Kumar, “Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-hoc Networks”, International Journal of Computer Network and Information Security, Volume 3, pages 39-46, 2013.

C.M barushimana, A.Shahrabi, “Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks,” Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, (2003).

Wang, Weichao, Yi Lu, and Bharat Bhargava. "On security study of two distance vector routing protocols for mobile ad hoc networks." In Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.(PerCom 2003)., pp. 179-186. IEEE, 2003.

Tseng Y.C., Shen C.C, and Chen W.T. Mobile ip and ad hoc networks: An integration and implementation experience. Technical report, Dept. of Comput. Sci.and Inf. Eng., Nat. Chiao Tung Univ., Hsinchu,, Taiwan, 2003.

AnkurKhetrapal, “Routing Techniques for Mobile Adhoc Networks Classification Qualitative/Quantitative Analysis,” Proceedings of ICWN, pp. 251-257, 2006.

Chen, Tsu-Wei, and Mario Gerla. "Global state routing: A new routing scheme for ad-hoc wireless networks." *Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on*. Vol. 1. IEEE, 1998.

Iwata, Atsushi, et al. "Scalable routing strategies for ad hoc wireless networks." *IEEE journal on selected areas in communications* 17.8 (1999): 1369-1379.

Yi, Ping, et al. "A new routing attack in mobile ad hoc networks." *International Journal of Information Technology* 11.2 (2005): 83-94.

Guo, Yinghua, Steven Gordon, and Sylvie Perreau. "A flow based detection mechanism against flooding attacks in mobile ad hoc networks." *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*. IEEE, 2007.

Desilva, Saman, and Rajendra V. Boppana. "Mitigating malicious control packet floods in ad hoc networks." *Wireless Communications and Networking Conference, 2005 IEEE*. Vol. 4. IEEE, 2005.

HarikrishnanNair, Sreeja Nair,”Firewall based Signature Enhancement for flooding attack in MANET”, International journal of advanced Research in computer and communication Eng.,March 2016.

Neethu Raj, P., S. Suresh Babu, and N. Nishanth. "A Novel Syn Flood Detection Mechanism for Wireless Network."

Saetang, Watchara, and Sakuna Charoenpanyasak. "CAODV free blackhole attack in ad hoc networks." *International Conference on Computer Networks and Communication*

Systems. Vol. 35. No. 2. 2012.

Sen, Jaydip, Sripad Koilakonda, and Arijit Ukil. "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks." *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*. IEEE, 2011.

Wei, Chen, et al. "A new solution for resisting gray hole attack in mobile ad-hoc networks." *Communications and Networking in China, 2007. CHINACOM'07. Second* International Conference on. IEEE, 2007.

Gonzalez Duque, Oscar Fredy, et al. "Detection and accusation of packet forwarding misbehavior in mobile ad-hoc networks." Journal of Internet Engineering 2.1 (2008).

Pu, Cong, Sunho Lim, Jinseok Chae, and Byungkwan Jung. "Active detection in mitigating routing misbehavior for MANETs." Wireless Networks 25, no. 4 (2019): 1669-1683.

Delkesh, Taher, and Mohammad Ali Jabraeil Jamali. "EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs." Journal of Ambient Intelligence and Humanized Computing 10, no. 5 (2019): 1897-1914.

Veeraiah, Neenavath, and B. Tirumala Krishna. "Trust-aware FuzzyClus-Fuzzy NB: intrusion detection scheme based on fuzzy clustering and Bayesian rule." Wireless Networks 25, no. 7 (2019): 4021-4035.

Jhaveri, Rutvij H. "MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs." Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on. IEEE, 2013.

Schweitzer, Nadav, et al. "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks." IEEE Transactions on Mobile Computing (2016).

Panda, Niranjan, and Binod Kumar Pattanayak. "Analysis of Blackhole Attack in AODV and DSR." International Journal of Electrical and Computer Engineering 8.5 (2018): 3093.

Panda, Niranjan, and Binod Kumar Pattanayak. "Defense against co-operative black-hole attack and gray-hole attack in MANET." Int. J. Eng. Technol 7.3.4 (2018): 84-89.

Hu, Y-C., Adrian Perrig, and David B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks." INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 3. IEEE, 2003.

Perrig, Adrian, and J. D. Tygar. "Tesla broadcast authentication." Secure Broadcast Communication. Springer US, 2003. 29-53.

Van Phuong, Tran, et al. "Transmission time-based mechanism to detect wormhole attacks." *Asia-Pacific Service Computing Conference, The 2nd IEEE*. IEEE, 2007.

Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff. "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks." *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*. IEEE, 2005.

Mokube, Iyatiti, and Michele Adams. "Honeypots: concepts, approaches, and challenges." *Proceedings of the 45th annual southeast regional conference*. ACM, 2007.

Qian, Lijun, Ning Song, and Xiangfang Li. "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path." *Wireless Communications and Networking Conference, 2005 IEEE*. Vol. 4. IEEE, 2005.

Yun, Ji-Hoon, et al. "Wodem: Wormhole attack defense mechanism in wireless sensor

networks." *Ubiquitous Convergence Technology*. Springer, Berlin, Heidelberg, 2007. 200-209.

Choi, Sun, et al. "WAP: Wormhole attack prevention algorithm in mobile ad hoc networks." *Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on*. IEEE, 2008.

Biswas, Juhi, Ajay Gupta, and Dayashankar Singh. "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol." *Industrial and Information Systems (ICIIS), 2014 9th International Conference on*. IEEE, 2014.

Chaurasia, Umesh Kumar, and Varsha Singh. "MAODV: Modified wormhole detection AODV protocol." *Contemporary Computing (IC3), 2013 Sixth International Conference on*. IEEE, 2013.

Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Rushing attacks and defense in wireless ad hoc network routing protocols." *Proceedings of the 2nd ACM workshop on Wireless security*. ACM, 2003.

Papadimitratos, Panagiotis, and Zygmunt J. Haas. "Secure message transmission in mobile ad hoc networks." Ad Hoc Networks 1.1 (2003): 193-209.

Kannhavong, Bounpadith, et al. "Analysis of the node isolation attack against OLSR-based mobile ad hoc networks." Computer Networks, 2006 International Symposium on. IEEE, 2006.

Dhillon, Danny, et al. "Implementation & evaluation of an IDS to safeguard OLSR integrity in MANETs." Proceedings of the 2006 international conference on Wireless communications and mobile computing. ACM, 2006.

Douceur, John R. "The sybil attack." *International Workshop on Peer-to-Peer Systems*. Springer, Berlin, Heidelberg, 2002.

Hashmi, Saorsh, and John Brooke. "Towards sybil resistant authentication in mobile ad hoc networks." *Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on*. IEEE, 2010.

Abbas, Sohail, et al. "Lightweight sybil attack detection in manets." IEEE systems journal 7.2 (2013): 236-248.

Piro, Chris, Clay Shields, and Brian Neil Levine. "Detecting the sybil attack in mobile ad hoc networks." Securecomm and Workshops, 2006. IEEE, 2006.

Lin, Xiaodong, et al. "ASRPAKE: An anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks." Communications, 2007. ICC'07. IEEE International Conference on. IEEE, 2007.

Gada, Dhaval, et al. "A distributed security scheme for ad hoc networks." Crossroads 11.1 (2004): 5-5.

Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

Ramanujan, Ranga, et al. "Techniques for intrusion-resistant ad hoc routing algorithms (TIARA)." *MILCOM 2000. 21st Century Military Communications Conference Proceedings*. Vol. 2. IEEE, 2000.

Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks." *Proceedings of the 6th annual international conference on Mobile computing and*

networking. ACM, 2000.

Kong, Jiejun, et al. "A secure ad-hoc routing approach using localized self-healing communities." *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005.

Nasser, Nidal, and Yunfeng Chen. "Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks." *Communications, 2007. ICC'07. IEEE International Conference on*. IEEE, 2007.

Morris Dworkin, "NIST, Special Publication SP 800–38A Recommendations for Block Cipher Modes of Operation, Methods and Techniques", *National Institute of Standards and Technology*, December 2001.

Wegman, Mark N., and J. Lawrence Carter. "New hash functions and their use in authentication and set equality." Journal of computer and system sciences 22.3 (1981): 265-279.

Zapata, Manel Guerrero, and Nadarajah Asokan. "Securing ad hoc routing protocols." Proceedings of the 1st ACM workshop on Wireless security. ACM, 2002