VARIOUS ATTACKS AND COUNTERMEASURES IN MOBILE AD HOC NETWORKS: A SURVEY

Elina Pattanaik[1] Himanshu Bhusan Mohapatra[2]
[1] *Computer Science Engineering, Gandhi Engineering College, Bhubaneswar (GEC, Bhubaneswar), India*
[2] *Electronics & Communication Engineering, Gandhi Engineering College, Bhubaneswar (GEC, Bhubaneswar), India*

***Abstract:*—A Mobile ad hoc network (MANET) is self organizing multi-hop network. In general MANET is characterized by the open wireless medium and very open to anyone. Due to the unique characteristics such as dynamic network topology, limited bandwidth, limited battery power and infrastructure less network environment, MANET is lacking in centralized authorization and highly vulnerable to malicious attacks. Thus the security is a critical problem when implementing MANET. In this survey, we have investigated different tools used by various attacks in MANET relating to fail routing protocols and described the mechanisms used by the secured routing protocols to counter them. The main objective of this paper is to present an extensive survey of the known attack detection, prevention approaches and to present new dimensions for their classification.**

Keywords — Routing protocol; Security; Attacks; MANET; Vulnerability; Active; Passive; Malicious; AODV; DSR; OLSR; RREQ; RREP.

1. INTRODUCTION

MANET is a self configured network consists of mobile nodes that communicate through a wireless medium in the lack of any centralized control of the network **[1].** Each node can travel about freely in space. Therefore, the topology of the network changes dynamically a MANET can be constructed quickly at a low cost. MANET has a dynamic topology such that nodes can easily join or leave the network at any instance. They have many possible applications, mainly, in military and rescue areas such as linking soldiers on the battlefield or creating a new network in place of a network which collapsed after a disaster like an earthquake and flood.

ROUTING PROTOCOLS IN MANET

Currently, numerous efficient routing protocols have been proposed. It can be classified into three categories, such as reactive, proactive and hybrid.

Proactive protocols: Proactive protocols are called table-driven protocols; includes destination sequenced distance vector (DSDV) protocols and Optimized Link State Routing Protocol (OLSR) **[2, 3].** In this type of protocols, each node maintains its own routing table and update by periodically exchanging routing messages with other nodes.

Reactive protocols: Reactive protocols are called on demand protocols; includes Adhoc on-demand distance vector (AODV) **[4, 5, 6]** and dynamic source routing (DSR) protocols **[7].** In reactive routing schemes, each node searches for a route, only when needed, to establish a connection with other nodes to accomplish data transfer.

Hybrid routing protocols: Hybrid routing protocols such as core extraction distributed ad-hoc routing (CEDAR) protocol **[8],** combine the best features of both reactive and proactive protocols. It uses reactive approach when the destination is within the range and applies proactive approach when the destination is outside the range. The routing protocols relay on carry between nodes owed to the lack of a centralized administration and believe that all nodes are truthful and well-behaved. A malicious node can start routing attacks to disturb routing operations, or denial-of-service attacks **[9]** to provide refuse services to legitimate nodes.

CHARACTERISTICS OF ATTACKS

Nature of attacks: An attack is one of the events which aim at compromising the security of the network. They are many and varied in these MANET which aimed at disrupting the operation of the network. The malicious nodes come in the way and interrupt the normal function of the network.

Active attacks: Active attacks are actively altering the data with the intention to obstruct the operation of the targeted networks. Such attacks include actions as communication modifications, message replays, message fabrications and the denial of service (DoS) attacks. Active attacks were characterized by route disruption, route incursion, node segregation and resource consumption **[9].**

Passive attacks: Passive attacks do not plan to disturb the network operations; they are launched to steal important information in the targeted networks. Eavesdropping attacks and traffic analysis attacks are examples of passive attacks. Identifying this kind of attack is not easy because neither the system resources nor the critical network functions are physically affected to confirm the intrusions.

Internal attacks: Internal attacks are form compromised nodes that are actually part of the network. The adversaries are already part of the network as authorized nodes. Internal attackers are more severe and difficult to detect when compared to external attacks

External attacks: External attacks are carried out by the nodes that do not belong to the network. It can be prohibited by using standard security mechanisms such as encryption method.

Single and multiple attackers: Attackers may initiate attacks against the ad hoc networks independently or by colluding with the other attackers. Single attackers in general build a moderate traffic load as long as they are not capable to attain any wired facilities. Because they also have similar abilities to the other nodes in the networks, their controlled resources become the fragile points to them. Though, if many attackers are colluding to launch attacks, protecting the ad hoc networks against them will be complicated. Colluding attackers may simply shut down any single node in the network and be capable to degrading the efficiency of network's distributed operations including the security mechanisms. Adding to the severity, colluding attackers could be widely distributed or reside at the certain area where they presumed high communication rate in the networks exist. If no suitable security measures used, nodes in that targeted area are prone to any kind of DoS attacks that could be launched by the colluding attackers **[10].**

2. SECURITY IN AD HOC WIRELESS NETWORK

Ad hoc wireless networks are highly vulnerable to security attacks compared to wired networks or infrastructure based wireless network. Security in MANET can be generally classified into data security and route security. In data security, data is protected against any type of unauthorized disclosure, disruption and destruction. In route security, routing (packet forwarding) is protected against any type of deception. Solving all vulnerabilities related to both route and data securities realize both data integrity and confidentiality.

Requirements of network security: A security protocol for ad hoc wireless networks should satisfy the confidentiality, integrity, availability and non-repudiation.

TYPES OF ATTACKS

Different types of attacks are possible in MANET **[11-20].** But all the attacks are affecting the functioning of network. In this section significance and mechanism of various types of attacks are discussed in detail.

Wormhole attack: A wormhole attack **[21]** is a complicated and severe attack in MANET. A couple of colluding attackers record packets at one spot and replay them at another spot using a private high speed network. The importance of this attack is that it can be launched adjacent to all communications that give authenticity and confidentiality.

Black hole attack: In this attack the malicious node falsely advertises network path to the destination node during the path finding process or in the route update messages. The goal of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node disturbed.

Sinkhole attack: A sinkhole node tries to attract data to itself by convincing neighbors through broadcasting fake routing information and let them know itself on the way to particular nodes. During this procedure, sinkhole node attempts to draw all network traffic to itself. Thereafter it alters the data packet or drops the packet silently. It enhances network overhead, reduces network's life time by boosting energy consumption, finally destroy the network.

Rushing attack: In on demand routing protocol all intermediate nodes should forward only the first received route request from all route discovery & all further received RREQ are ignored. So, a malicious node just exploits this property of the process of route discovery by quickly forwarding RREQ packets in order to expand access to the forwarding group. As a result, source node will not be able to discover any suitable routes that do not include the malicious node **[22].**

Selfish attack: It mostly involves no collaboration for the fine performance of the network. It is possible to identify two kinds of nodes which do not wish to take part in the network. Faulty nodes which do not work perfectly and malicious, it is those which purposely, try to tackle the system attack on the reliability of the data, accessibility of the services, authenticity of the entities. Selfish nodes are those entities whose purpose is to make best use of their benefit **[23].**

Sibil attack: In this attack, the attacker weakens the reputation system of a peer-to-peer network by making a huge number of fake identities, using them to gain a disproportionately large influence. It can occur in a distributed system that operates without a central authority to verify the identities of each communicating entity. Because each entity is only aware of others through messages over a communication channel, a Sybil attacker can assume many different identities by sending messages with different identifiers.

Jamming attack: In this form of attack, goal of a jammer is to hinder with legitimate wireless communications and to corrupt the overall quality of service (QoS) of the network. This attack able to achieve this objective by either prevents a real traffic source from sending out a packet, or by preventing the party of legitimate packets to disturb communications.

Flooding attack: This type of attack sends a vast number of RREQ packets in an attempt to consume the network resources. The sender IP address is forged to a randomly selected node and the broadcast ID is purposely increased. It creates feasible for an adversary to carry out DoS by saturating the support with a number of distribution messages, by decreasing the output of nodes **[24].**

Link withholding attack: In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a cluster of nodes, which can effect in link loss to these nodes. This type of attack is mainly severe in the optimized link state routing (OLSR) protocol

Spoofing attack: In this type of attack, the identity of another node is steals by attacker, thus it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be initiated, which can critically cripple the network.

Replay attack: This type of attack, a malicious node records another nodes official message and resends them later. Consequently, other nodes to record their routing table with stale routes. This attack can be misused to imitate a specific node or simply to disturb and unwanted confusion in the routing process.

Colluding misrelay attack: In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing process in a MANET. This attack is hard to identify by using the usual methods such as watchdog and pathrater **[25].**

Byzantine attack: In this attack, a compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in interruption or degradation of the routing services.

Information disclosure attack: In this attack, a compromised node can leak secret or important information to unauthorized nodes in the network. Such information may comprise concerning the network topology, geographic position of nodes or optimal paths to the authorized nodes in the network.

Neighbor attack: In this attack, when the intermediate node receives a RREQ/RREP packet. The intermediate nodes add its own ID to the packet before forwarding it to next hop or node. But the malicious node forwards the packets without ID. In this case two nodes that are not in the communication range of each other believe that they are neighbors, resulting in a disrupted route operation. In neighbor attack, the malicious node does not capture the data packets from the source node **[26].**

Jelly fish attack: This attacker first needs to intrude into the multicast forwarding group. It then delays data packets unreasonably for some amount of time previous to forwarding them. This results in much high end-to-end delay and thus degrades the performance of real applications.

Greyhole attack: It is also known as routing misbehavior attack. It works in two phases. In first stage node advertises itself as having suitable route to destination while in second stage nodes drops intercept packets with firm probability **[27].**

Sleep deprivation attack: In a routing protocol, this attacker, attacks might be launch by flooding the destination node with unnecessary routing packets. For instance, sleep deprivation attackers could flood every node in the networks by sending a vast number of RREQ, RREP and RERR packets to the destination node. Hence, that particular node is incapable to participate in the routing mechanisms and is out-of-the-way to the other nodes in the networks **[23].**

Route falsification attack: In this attack, malicious node can works in both direction, source node to destination node during RREQ and destination to source during RREP. When source node sends request to destination node or when destination node or other node gives reply for request. In this case, malicious nodes falsify the RREQ or RREP packets to indicate an optimal path to the source for making huge portion of the traffic go through them. When the source selects the falsified route, the malicious nodes can crash data packets they receive mutely **[28].**

Fabrication attack: Fabrication attack is an active attack; it breaks authenticity by exposing itself to become the source entity. After become a part of the network it sends error message to other legal nodes to say the route is not accessible further. Consequently, other node will then update their table with this bogus information. Through this manner it drops the routing packets **[28].**

3. COUNTERMEASURES FOR VARIOUS ATTACKS

The conventional work focused on providing preventive schemes for MANET routing protocols. Many schemes are based on encryption or key management technique to prevent unauthorized malicious node from fusion network. A big disadvantage of this technique is that they launch a heavy traffic by load to swap and verify the key. It creates to be in terms of limited bandwidth, limited battery, and limited computational capabilities.

The attackers attack severely the route discovery mechanism and network operation in MANET. So currently, several routing protocols proposed for MANET. In the earlier survey of attacks in MANET, conventional solutions are proposed for different attacks. In this section, countermeasures of attacks such as wormhole, black hole, sinkhole, rushing attack, selfish, sybil, jamming, flooding, spoofing, withholding, reply and colluding misrelay are proposed based on routing implementation individually.

Countermeasures for wormhole attack: In an ad hoc network, several researchers have worked on pretending and detecting wormhole attacks specifically. To defend against them, some efforts have been put on hardware design and signal processing techniques the data bits are transferred in some special modulating method known only to the neighbor nodes, they are resistant to the closed wormholes **[29].**

RF watermarking **[29]** proposed a solution to protect the MANET from the wormhole. It modulates the radio waveform in a specific pattern to accomplish authentication. Both mechanisms will be compromised if the malicious nodes can precisely capture the signal patterns. Neither of them can stop half open or open wormholes**.** Another potential solution is to integrate the prevention methods into Intrusion Detection Systems (IDS) **[30].** The traffic monitoring module of IDS will find that the ends of wormholes act as packet sinks.

Hu, Perrig and Johnson **[31]** proposed an approach to detect closed wormholes is packet leash. The leash is the information added into a packet to limit its transmission distance. The location information and loosely synchronized clocks together confirm the neighbor relation in the geographical leashes. Each node, prior to sending a packet, append its current position and transmission time to it. The recipient nodes, on receiving of the packet, calculate the distance to the source and the time it took the packet to traverse the path. The recipient can apply this distance anytime information to deduce whether the received packet passed through a wormhole or not.

Another set of wormhole prevention techniques is based on the time of flight of individual packets proposed by Capkun et al **[32]**. In order to avoid the problem of using special hardware in packet leaches, a Round Trip Time (RTT) mechanism is proposed by Jane Zhen and Sampalli **[33]**. The RTT is the time that extends from the RREQ message sending time of a node A to RREP message receiving time from a node B. A will compute the RTT between A and all its neighbors. Because the RTT between two fake neighbours is higher than between two real neighbors. Hu and Vans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas in
[34]. In this technique, nodes use specific 'sectors' of their antennas to communicate with each other. Each couple of nodes has to examine the direction of received signals from its neighbour. Hence, the neighbor relation is set only if the directions of both pairs match.

Khalil et al **[35]** proposed a protocol for wormhole attack discovery in static networks, called LiteWorp. In this once deployed, nodes get full two-hop routing information from their neighbours. A wormhole detection mechanism based on statistical analysis of multipath routing proposed by Song et al **[36]**. They observes that a link formed by a wormhole is very attractive in routing sense, and will be preferred and requested with unusually high frequency as it only uses routing data already available to a node.

Abdesselam, Bensaou and Taleb **[37]** have presented an effective method for detecting and preventing wormhole attacks in OLSR. They use a simple four-way handshaking messages exchange to detect wormhole tunnels

Wormhole Attack Prevention (WAP) proposed by Choi, Kim, Lee, and Jung **[38]** not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. This has been achieved through the use of the neighbor node monitoring method of each node and wormhole route detection method of the source node on the selected route. This mechanism is implemented based on the DSR protocol. Shang, Laih and Kuo **[39],** proposed a technique of hop count analysis. In this method selects routes and "avoids" rather than "identify" the wormhole resulting in low cost and overhead.

The Trust Based Model by Jain and Jain **[40]** presents a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means.
Countermeasures for black hole attack: Black hole attack principally prevented by DRl table and cross checking scheme **[41, 42].**

Hesiri Weerasinghe **[43]** proposed an algorithm to identify collaborative Black hole attack. Herein the AODV routing protocol is little modified by adding an additional table i.e. Data Routing Information (DRI) table and crosschecking using Further Request (FREQ) and Further Reply (FREP). Time-based Threshold Detection Scheme **[44]** proposed by L Tamilselvan is based on an enhancement of the original AODV routing protocol. The main idea is setting timer for collecting the other request from other nodes after receiving the first request. It stores the packet's sequence number and the received time in a table named collect route reply table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value.

In detection, prevention and reactive AODV scheme (DPRAODV**) [45]** an additional check is done to find whether the RREP_seq_no value is higher than the threshold value as compared to standard AODV. If the RREP_seq_no value is higher than the threshold value, the node is considered to be malicious and that node is added to the black list. N Mistry **[46]** proposed a solution for analyzing and improving the security of AODV routing protocol against Black hole attack. This approach is principally modifies the working of source node only, by means of additional function Pre_Receive Reply. A table Cmg_RREP Tab, a variable malicious node and a new timer MOS WAIT_TIME are also added to the default AODV.

Neighborhood-based and routing recovery scheme **[47]** based on the neighbor set information; a method is designed to deal with the black hole attack, which has two parts: detection and response. In detection process, first step is collect neighbor set information and second step is to determine whether there exists a black hole attack. G. Trust Table Method **[48]** proposed a protocol modifies the behavior of the original AODV to include the following techniques: Every node is provided with a data structure referred as trust table. This table is responsible for holding the addresses of the reliable nodes.

The secure AODV protocol **[49]** is an enhancement of the AODV consisting of a key management subsystem where each node obtains public keys from the other nodes that are present in the network. Verification and validation are done by the association of the identity of the node and the public key. This is achieved by two important mechanisms, one being the use of digital signatures to authenticate the message fields and second being the use of hash functions to protect the hopcount information.

Tanu Preet Singh proposed Optimized Black Hole Detection and prevention Algorithm **[50],**

1. While transmission=complete loop.
2. Maintain table for path selected on start of transmission containing sequence number of node.
3. Send data to relaying node.
4. Receive acknowledgement and store the sequence number of node.
5. Look for sequence number received in the routing table.
6. If sequence number found then, authenticated transmission and continue.
7. Else node is unauthorized and it is black hole.
S. End of step one loop.
9. Exit.

Countermeasures for sinkhole attack: Sinkhole intrusion indicators technique (SIIT) makes use of two sinkhole detection indicators for MANET. The two indicators proposed here are sequence number discontinuity and route-add ratio. The series number discontinuity is calculated by the overall average difference between the current and the final sequence number from each node. The route-add ratio is the proportion of routes that traverse a particular node to the total number of routes added to this node's routing table.

Adaptive technique: A trust weight assigned by every ad hoc node to its neighbors. Throughout the transmission if a neighbor fails to transmit its message to a designated recipient, the ad hoc node then lesser the trust weight it has given to the neighbor. The neighbor then deducts the assigned weight of the next ad hoc node in the transmission path **[51].**

Cooperative technique: This technique makes use of three different kinds of packets sinkhole alarm packet (SAP), sinkhole detection packet (SDP) and sinkhole node packet (SNP). SAP will contains sinkhole route, series number of the fake RREQ, present sequence number of the node itself. Detection packet contains the common path, series number of bogus RREQ, network identity of itself. The nodes in the sinkhole path are not allowed to produce or forward an SDP. If any node gets an SDP from the nodes in the sinkhole path, it just rejects the packet and detaches the sender of the SDP from the network and in SNP to inform the network of sinkhole node. The SNP packet will contain the sinkhole node to the whole network unless it received an SNP for this sinkhole route from another node **[52].**

Collaborative technique: This method chiefly involves selection of single node as monitor node out of many where monitor node initiates detection process, based on the message that it receive during this process, each node determines node it suspect to be malicious and send votes to monitor node which upon carefully inspecting votes determine malicious node from the suspected nodes **[53].**

Cluster analysis technique: Cluster analysis is a data mining technique which works by grouping patterns which are similar to each other in single group and different from patterns in other groups. Herein cluster analysis is used to separate false RREQs from normal RREQs and to verify indicators for detection **[54].**

Countermeasures for rushing attack: One simple instance of the rushing attack is when an attacker forwards a RREQ beyond the normal radio transmission range (for example by using a higher gain antenna or a higher power level), thus suppressing subsequent REQs from this route discovery.

Secure neighbor detection: It allows both the sender and the receiver of a RREQ to verify that the other party is within the normal direct wireless communication range.

Requirements for secure neighbor detection: Introducing two nodes that are not within the maximum transmission range as neighbors; and **[55]** claiming that it is a neighbor of another node without being able to hear packets directly from that node

Our secure neighbor detection protocol: It presents a secure Neighbor Detection protocol that allows both the initiator and the responder to check that the other is within a maximum communication range.

Integration with an on-demand protocol: In an on-demand protocol, neighbor verification is performed during each Route Discovery.

Secure route delegation: In RREQ propagation, to enable each node to verify that all the secure neighbor detection steps were performed between any adjacent pair of nodes in the REQUEST, i.e., verify that both nodes of each adjacent node pair indeed believes to be a neighbor.

Randomized message forwarding: The secure neighbor detection and secure route delegation techniques are not sufficient to find the rushing attack, since an adversary can still get an advantage by forwarding RREQ very rapidly. It uses a random selection technique to minimize the chance that a rushing adversary can dominate all returned routes. Hence there are two parameters in randomized forwarding technique: (1) the number of REQUEST packets to be collected and (2) the algorithm by which timeouts are selected.

Secure route discovery: In this section describe three techniques in concert to prevent the rushing attack: secure Neighbor Discovery protocol, secure Route Delegation and delegation acceptance protocol. Randomized selection of which RREQ will be forwarded.

Integrating secure route discovery with DSR: To integrate rushing prevention with DSR **[56]** or other secure protocols based on DSR, Route Discovery frequency is limited as in Ariadne **[57].** Each time a node forwards a RREQ, it first performs a Secure Neighbor Detection exchange with the previous hop. When it forwards the REQUEST, it includes in the REQUEST a bidirectional Neighbor Verification for the previous hop. As in DSR, the target of a Route Discovery returns a RREP for each distinct RREQ it receives. Each such RREP is sent with a source route selected by reversing the route in the RREQ. This route is likely to work if there are no attackers on the route, since Neighbor Detection only finds bidirectional neighbors.

Integrating secure route discovery with AODV: In AODV **[58],** as well as other secure protocols based on AODV **[59, 60],** RREQ packets do not carry a node list. However, in order to filter excessive malicious RREQs, each RREQ to carry a node list is required. Instead of forwarding the first RREQ received, nodes using our Secure Route Discovery randomly select one of the first n RREQs it receives and treats it as the RREQ **[61]** to forward. More specifically, it places the initiator of the Route Discovery in its routing table using the previous hop of the RREQ selected as the next-hop destination. It then appends its address and authentication information to the node list, and forwards it as in DSR

Integrating secure route discovery with secure Ad Hoc: When using rushing attack prevention together with a secure on-demand routing protocol, a node can first attempt Route Discovery using that secure protocol. If a rushing attacker prevents the discovery of any working routes, the node can then set a flag indicating that it wants to use rushing attack prevention, though it must also authenticate that flag to prevent modification.

Countermeasures for selfish attack: Objective of this is to find out the malicious node that performs the DOS by selfish node in network.

Assumption algorithm to design selfish node detection [62]:

1. A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2. Every node has a unique identity in the network, which is allocated to a new node jointly by existing nodes.
3. The source node creates mobile agent after a specific period of time.
4. The mobile agent moves towards forward path created using RREQ and RREP.
5. The agent calculates the packet receive and forward by a node.
6. If the agent finds out a malicious node, instead of moving onward, it sends a report to the source node. **Countermeasures for sybil attack:** Douecer has shown that a Sybil attacker cannot be prevented by tests of finite resources **[63].** However, unlike separate entities, all identities of a Sybil attacker must share the same set of resources, and this sharing can be identified in some situations **[64].**

In the mobile environment, a single entity imitating multiple identities has an important constraint that can be detected: because all identities are part of the same physical device, they have to move in union, while independent nodes are free to move. when nodes move geographically, all the Sybil identities will show or disappear at the same time as the attacker moves in and out of range. Assuming an attacker uses a single-channel radio, must transmit serially, whereas multiple independent nodes multiple Sybil identities can transmit in parallel. The latter two differences form the basis of the Sybil attack finding scheme proposed here. A single attacker with multiple radios will not be identified as such; however, there may be analogous methods for detecting multi-radio sybil attackers.

Countermeasures for jamming attack: Wood et al. proposed that no effective defense was yet known against link-layer jamming **[65].** Both Stahlberg **[66]** and Wood et al. quote how an attacker might keep sending RTS packets to elicit CTS packets from its victims. Negi and Perrig **[67]** investigate the attack of a jammer that identify and jams RTS packets, in addition to sends RTS packets to reserve the largest time interval possible, using the Poisson arrival model. Konorski **[68]** proposes a scheduling policy that addresses the selfish behavior of using small or no contention time (also called random backoff time) in contention-based protocols, in the context of single-hop networks and multi-hop networks.

Kyasanur et al. **[69]** proposes the sender set the contention time; the receiver sets and sends the time in the CTS and ACK packets to the sender. The sender uses this assigned contention time in the subsequent transmission to the receiver. The receiver can then tell if the sender is being selfish using a value smaller than the assigned value, by observing the number of idle slots between consecutive transmissions from the sender. Cagalj et al. **[70]** studied the effect of a group of selfish cheaters from a game-theoretic point of view. When focusing DoS attacks, in which the purpose of the misbehaving party lies in disruption instead of getting more bandwidth. Different countermeasures are thus required.

Countermeasures for flooding attack: P. Yi et al. **[71],** proposed a simple mechanism to avoid the flooding attack in the AODV routing protocol. In this approach, every node should be monitors and calculates the rate of its neighbors' RREQ. If any neighbor RREQ rate exceeds the predefined threshold, the node records the ID of that neighbor in a blacklist. Then, the black list node does not send futures RREQs.

Two constraint of this mechanism: First this node cannot prevent against of this attack in which the flooding rate is under the threshold. Second if a malicious node impersonates the ID of a legitimate node and broadcast a huge number of RREQs, other nodes may put the ID of this legitimate node on the blacklist in mistake. S. Desilva, and R. V. Boppana, **[72],** proposed an adaptive technique to moderate the effect of a flooding attack. This approach is based on statistical analysis to identify malicious RREQ flood and avoid the forwarding packets. In this approach, similar to **[71],** each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the predetermined time. The RREQs from a source whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in **[70],** where the threshold is set to be fixed, this approach determines the threshold based on a statistical study of RREQs. The key benefit of this approach is that it can decrease the impact of the attack for varying flooding rates.

Countermeasures for message withholding attack:

By withholding a Topology control (TC) message in OLSR **[73],** a false node can remove a specific node and stop it from receiving data packets from other nodes. After analyzing and evaluating the impact of this kind of attack in detail, the researchers proposed a finding technique based on observation of both a TC message and a HELLO message generated by the Multipoint

relay (MPR) nodes. If a node does not hear a TC message from its MPR node regularly but hears only a HELLO message, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes.

Similarly, in **[74],** the authors proposed an intrusion detection system to detect TC link and message withholding in the OLSR protocol. In this approach, each node observes whether an

MPR node generates a TC message often or not. In case an MPR node produces a TC message regularly, the node checks whether or not the TC message actually contains itself to detect the attack.

The main draw back of these approaches are that they cannot detect the attack that is launched by two colluding consecutive nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

Countermeasures for link spoofing attack: To detect a link spoofing attack, D. Raffo **[75]** proposed a location information-based detection method by using cryptography with a Global Positioning System (GPS) and a time stamp. It requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes. This approach detects the link spoofing by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maximum transmission range.

The main drawback of this approach is that it might not work in a situation where all MANET nodes are not set with a GPS. Moreover, attackers can still advertise false information and make it hard for other nodes to detect the attack. B. Kannhavong et al **[76]** show that a malicious node that advertises fake links with a target's two-hop neighbors can effectively make the target choose it as the only MPR. During simulations, they confirm that link spoofing can have a devastating impact on the target node. Then, they present a technique to detect the link spoofing attack by adding two-hop information to a HELLO message. Especially, the proposed solution needs each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the link spoofing attack is launched. The main advantage of this approach is that it can detect the link spoofing attack without using special hardware such as a GPS or requiring time management. One constraint of this approach is that it might not identify link spoofing with nodes further away than three hops.

Countermeasures for replay attack: C. Adjih, D. Raffo **[77],** proposed a solution to protect a MANET from a replay attack by using a time stamp with the use of an asymmetric key. This result in prevents the replay attack by comparing the current time and time stamp contained in the received message. If the time stamp is too far from the current time, the message is judged to be doubtful and is discarded. Even

though this solution works well against the replay attack, it is still susceptible to a wormhole attack where two colluding attackers use a high-speed network to replay messages in a far-away location with no delay.

Countermeasures for colluding misrelay attack: A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the network require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient. Z. Karakehayov **[78],** proposes a method to detect an attack in which multiple malicious nodes attempt to drop packets by requiring each node to tune their transmission power when they forward packets. As an example, the author studies the case where two colluding attackers drop packets. The proposed solution requires each node to increase its transmission power twice to detect such an attack. However, this approach might not detect the attack in which three colluding attackers work in collusion. In general, the main draw back of this approach is that even if we require each node to increase transmission power to be P times, we still cannot detect the attack in which P+1 attackers work in collusion to drop packets. Therefore, further work must be done to counter against this type of attack efficiently.

4. CONCLUSIONS

In this survey, current-state-of-the-art of routing attacks and countermeasures in a MANET is reviewed comprehensively. Advantages and disadvantages of MANET elucidate in detail. It shows that even though many solutions have been proposed, they still are not perfect in terms efficiency. Although some solutions are performing well in the presence of one fake node, they may not be applicable to multiple colluding attackers. Some other solutions may need unique hardware or an improvement of the existing protocol. Further in this survey more attention paying on developing the effectiveness of the security schemes by applying symmetric and asymmetric cryptography with cost effective.

REFERENCES

[1] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting Blackhole Attack on AODV-based Mobile Ad HocNetworks by Dynamic Learning Method. International Journal, 5(3),338-346.

[2] Th. Clausen et al., "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietf-manet-olsr-11.txt,July 2003.

[3] Ibm, C., & Perkins, W. E. (1994.). Highly Dynamic (DSDV) for Mobile Computers Routing. Methods, 234-244.

[4] Singh, P. K. (2012). An Efficient Prevention of Black Hole Problem inAODV Routing Protocol in, 902-906.

[5] E. A. M. P. M. (2009). Trust Based Secure Routing in AODV Routing Protocol. Information Sciences, 0-5.

[6] Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applicationsby Subir Kumar Sarkar, T G Basavaraju C Puttamadappa. Johnson, D. B., &Maltz, D. A. (2001). DSR : The Dynamic SourceRouting Protocol for Multi-Hop Wireless Ad Hoc Networks. Discovery, 1-25.

[7] P. Sinha, R. Sivakumar and V. Bharghavan, "CEDAR: A Core ExtractionDistributed Ad Hoc Routing Algorithm", IEEE Journal on SelectedAreas in Communications, Vol. 17, No. 8, August 1999, pp. 1454-1466.

[8] Alikhany, M., Abadi, M.: A Dynamic Clustering Based Approch For AnomalyDetection In AODV Based MANET. In: International Symposium on ComputerNetwork & Distributed System. IEEE (2011).

[9] Razak, S.A., Furnell, S.M., Brooke, P.J.: Attacks against Mobile Ad Hoc Networks Routing Protocols, Network Research Group, University of Plymouth, Devon.Chandraprabha Rawat," A Review: Wormhole attack In Mobile Ad Hoc Network.", IJARCCE,Vol. 2, Issue 3,pp.1358_ 1362, March 2013.

[10] Kishor Jyoti Sarma, Rupam Sharma, Rajdeep Das "A Survey of Black Hole Attack Detection in Manet",pp.202_205, 2014.

[11] Ahmed Sherif , Maha Elsabrouty and Amin Shoukry, "A Novel Taxonomy of Black-hole Attack DetectionTechniques in Mobile Ad-Hoc Network (MANET)"pp.346_352, 2013.

[12] Yee Wei Law, Lodewijk van Hoesel, Jeroen Doumen, Pieter Hartel PaulHavinga"EnergyEfficientLinkLayerJammingAttacks againstWireless Sensor NetworkMAC Protocols", pp76_88,November 7, 2005.

[13] Y.C. Hu, Adrian Perrig, David B. Johnson ,"Rushing Attacks and Defense in Wireless Ad Hoc NetworkRouting Protocols"pp.30_40, September 19, 2003.

[14] Debdutta Barman Roy, Rituparna Chaki, A. Özcan, J. Zizka, and D. Nagamalai "Detection of Denial of Service Attack Due to Selfish Nodein MANET by Mobile Agent" pp. 14–23, 2011.

[15] Gandhewar.N and Rahila Patel "Review on Sinkhole Detection Techniques in Mobile Ad hoc Network "K. Deep et al. (Eds.): Proceedings of the International Conference on SocProS 2011, AISC 130, pp. 535–548.

[16] Kannhavong.B, Nakayama.B, Nemoto.Y, And Kato.N, "A survey of routing attacks in mobile ad hoc networks" pp.85_91, October 2007.

[17] Chris Piro, Clay Shields, Brian Neil Levine "Detecting the Sybil Attack in Mobile Ad hoc Networks" pp.1_11,2006.

[18] Preeti Nagrath, Bhawna Gupta," Wormhole Attacks in Wireless Ad hoc Networks and their Counter Measurements:A Survey"pp.245_250,2011.

[19] Sharma, S.C., Mamatha, G.S.: Network Layer Attacks and Defense Mechanisms inMANETS- A Survey. International Journal of Computer Applications (0975–8887)9(9) (November 2010).

[20] Shim, W., Kim, G., Kim, S.: A distributed sinkhole detection method using cluster analysis. Expert Systems with Applications (2010).

[21] Konate, K., Abdourahime, G.: Attack Analysis in mobile Adhoc network Modelingand Simulation. In: Second International Conference on Intelligent Systems. IEEE(2011).

[22] Manikandan, K.P., Satyaprasad, R.: A Survey on Attacks and Defense Metrics ofRouting Mechanism in Mobile Ad hoc Networks. International Journal of AdvancedComputer Science and Application (IJACSA) 2(3) (March 2011).

[23] S. Marti et al., "Mitigating Routing Misbehavior inMobile Ad Hoc Networks," 6th MobiCom, Boston, MA,Aug. 2000.

[24] Alikhany, M., Abadi, M.: A Dynamic Clustering Based ApprochFor

[25] Anomaly Detection In AODV Based MANET. In: International Symposium on ComputerNetwork & Distributed System. IEEE (2011).

[26] Manikandan, K.P., Satyaprasad, R., Rajasekhararao: Analysis and Diminution ofSecurity Attacks on Mobile Ad hoc Network. IJCA Special Issue on "Mobile AdhocNetworks" MANETs (2010).

