International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012

http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

ATTACKS IN MOBILE AD HOC NETWORKS

Dr. Mukta Makhija
Professor, Department of Computer Application,
Inmantec Institutions, Ghaziabad,
Uttar Pradesh, India.
drmuktamakhija20@gmail.com

Abstract

A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using various cryptographic techniques to counter measure the routing attacks against MANET. However, these mechanisms are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. In this paper, the current security issues in MANET are investigated. Particularly, we have examined different routing attacks, such as flooding, black hole, link spoofing, Wormhole, and colluding misrelay attacks, as well as existing solutions to protect MANET protocols.

Keywords: MANET Security, Routing Protocols, Cryptography, Communications and Data Security, Shared, Wireless Channel.

1. Introduction

A MANET is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. Due to self-organize and rapidly deploy capability, MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other. Security-sensitive computing environments. There are 15 major issues and sub-issues involving in MANET such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and Standards/products. Currently, the routing, power management, bandwidth management, radio.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

Interface and security are hot topics in MANET research. Although in this paper we only focus on the routing protocols and security issues in MANET. The routing protocols in MANET may generally be categorized as: table-driven/proactive and source-initiated (demand-riven)/reactive.

In proactive routing protocols, such as the optimized link state routing (OLSR) , nodes obtain. Routes by periodic exchange of topology information. In reactive routing protocols, such as the adhoc on demand distance vector (AODV) protocol , nodes find routes only when required. The overall goal of the security solutions for MANET is to provide security services including authentication, confidentiality, integrity, anonymity, and availability to the mobile users. In order to achieve to this goal, the security solution should provide complete protection spanning the entire protocol stack. We can categories MANET security in 5 layers, such as Application layer, Transport layer, Network layer, Link layer, and Physical layer. However, we only focus on the network layer, which is related to security issues to protect the ad hoc routing and forwarding protocols. From the security design perspective, the MANETs have no clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad hoc routing protocols, such as (AODV), (DSR) , and wireless MAC protocols, such as 802.11 , typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by Intentionally disobeying the protocol specifications. Recently, several research efforts introduced to counter against these malicious attacks. Most of the previous work has focused mainly on providing preventive schemes to protect the routing protocol in a MANET. Most of these schemes are based on key management or encryption techniques to prevent unauthorized nodes from joining the network. In general, the main drawback of these approaches is that they introduce a heavy traffic load to exchange and verify keys, which is very expensive in terms of the bandwidth-constraint for MANET nodes with limited battery and limited computational capabilities. The MANET protocols are facing different routing attacks, such as flooding, black hole; link withholding, link spoofing, replay, wormhole, and colluding misrelay attack. A comprehensive study of these routing attacks and countermeasures against these attacks in MANET can be found in the rest of this paper is organized as follows. In next section, we discuss routing protocols in MANET. Section 3 discusses current routing attacks as well as countermeasures against such attacks in existing MANET protocols.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

2. Routing Protocols in Manet

MANET routing protocols can be categorized into 2 classes as: table-driven/proactive and
Source-initiated (demand-driven)/reactive. In the following sections, we present the overview of these protocols.

2.1 Table-Driven Routing Protocols

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. The following sections discuss some of the existing table-driven ad hoc routing protocols.

2.1.1 Destination-Sequenced Distance-Vector (DSDV)

The Destination-Sequenced Distance-Vector (DSDV) routing protocol is a table-driven algorithm based on Bellman-Ford routing mechanism . The improvements made by to the Bellman-Ford algorithm include freedom from loops in routing tables. In DSDV every node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain table consistency. To help alleviate the potentially large amount of network traffic that such updates can generate, route updates can employ two possible types of packets: full dump and smaller *incremental* packets. Each of these broadcasts should fit into a standard-size of network protocol data unit (NPDU), thereby decreasing the amount of traffic generated. The mobile nodes maintain an additional table where they store the data sent in the incremental routing information packets. New route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination, as well as a new sequence number unique to the broadcast. The route labeled with the most recent sequence number is always used. In the event that two updates have the same sequence Number, the route with the smaller metric is used in order to optimize (shorten) the path. Mobiles also keep track of the settling time of routes, or the weighted average time that routes to a destination will fluctuate before the route with the best metric is received. By delaying the broadcast of a routing update by the length of the settling time, mobiles can reduce network traffic and optimize routes by eliminating those broadcasts that would occur if a better route was discovered in the very near future.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

2.1.2 Optimized Link State Routing (OLSR) Protocol

Optimized link state routing (OLSR) protocol is a proactive routing protocol and based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs. Generally, two types of routing messages are used in the OLSR protocol, namely, a HELLO message and a topology control (TC) message. A HELLO message is the message that is used for neighbor sensing and MPR selection.

In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically.

A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network. For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages. In OLSR, a node selects its MPR set that can reach all its two-hop neighbors. In case there are multiple choices, the minimum set is selected as an MPR set.

2.1.3 Wireless Routing Protocol (WRP)

Wireless routing protocols (WRP) is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. WRP is a loop free routing protocol. Each node maintains 4 tables: distance table, routing table, linkcost table & message retransmission list table. Link changes are propagated using update messages sent between neighboring nodes.

Hello messages are periodically exchanged between neighbors. This protocol avoids count-toinfinity problem by forcing each node to check predecessor information.

2.1.4 Clusterhead Gateway Switch Routing (CGSR) Protocol

Clusterhead gateway switch routing (CGSR) protocol is based on a cluster multihop mobile wireless network with several heuristic routing schemes. The authors state that by having a cluster head controlling a group of ad hoc nodes, a framework for code separation (among clusters), channel access, routing, and bandwidth allocation can be achieved. A cluster head selection algorithm is utilized to elect a node as the cluster head using a

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

distributed algorithm within the cluster. However, frequent cluster head changes can adversely affect routing protocol performance since nodes are busy in cluster head selection rather than packet relaying. Hence, instead of invoking cluster head reselection every time the cluster membership changes, a Least Cluster Change (LCC) clustering algorithm is introduced. Using LCC, cluster heads only change when two cluster heads come into contact, or when a node moves out of contact of all other cluster heads. CGSR uses DSDV as the underlying routing scheme, and hence has much of the same overhead as DSDV. However, it modifies DSDV by using a hierarchical cluster-head-to-gate-way routing approach to route traffic from source to destination. Gateway nodes are nodes that are within communication range of two or more cluster heads. A packet sent by a node is first routed to its cluster head, and then the packet is routed from the cluster head to a gateway to another cluster head, and so on until the cluster head of the destination node is reached. The packet is then transmitted to the destination.

2.2 On demand-driven reactive protocols

On demand protocols create routes only when desired by source nodes. When a Node requires a route to destination, it initiates route discovery process within the network. This process is completed once a route is found or all possible route permutations are examined. Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired.

2.2.1 Ad Hoc On-Demand Distance Vector (AODV)

AODV is an improvement of DSDV algorithm previously described. It is typically Minimizes the number of required broadcasts by creating routes on a demand basis, while DSDV algorithm maintain a complete list of routes. The authors of AODV classify it as a pure on demand route acquisition system, since nodes that are not on a selected path do not maintain routing acquisition or participate in routing table exchanges. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination Node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send An RREP to the source node.

2.2.2 Dynamic Source Routing (DSR)

Dynamic source routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broad- casting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record. A route reply is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken.

2.2.3 Temporary-Ordered Routing Algorithm (TORA)

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive loop-free distributed routing algorithm based on the concept of link reversal. TORA is proposed to operate in a highly dynamic mobile networking environment. It is source initiated and provides multiple routes for any desired source/destination pair. The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain routing information about adjacent (one-hop) nodes. The protocol performs three basic functions: route creation, route maintenance, and route erasure.

2.2.4 Relative Distance Micro Diversity Routing (RDMAR)

Relative Distance Micro diversity Routing (RDMAR) protocol estimates the distance between two nodes using the relative distance estimation algorithm in radio loops. RDMAR is a source initiated and having features similar to associatively based routing (ABR) protocol. RDMAR limits the range of route searching in order to save the cost of flooding a route request message into the entire wireless area. It is assumed in RDMAR that all ad hoc mobile hosts are migrating at the same fixed speed. This assumption can make good practical estimation of relative distance very difficult.

3. Routing Attacks in Manet

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

countermeasures against MANET protocols are discussed in detail.

3.1 Flooding Attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be Consumed and could lead to denial-of-service. A simple mechanism proposed to prevent the flooding attack in the AODV protocol. In this Approach, each node monitors and calculates the rate of its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake. In the authors show that a flooding attack can decrease throughput by 84 percent. The authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets.

Similar to, in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed, where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

3.2 Black hole Attack

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an Optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination Sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure 4 shows an example of a blackhole attack, where attacker a sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

other nodes' sequence numbers, the source node S will choose the route that passes through node A.

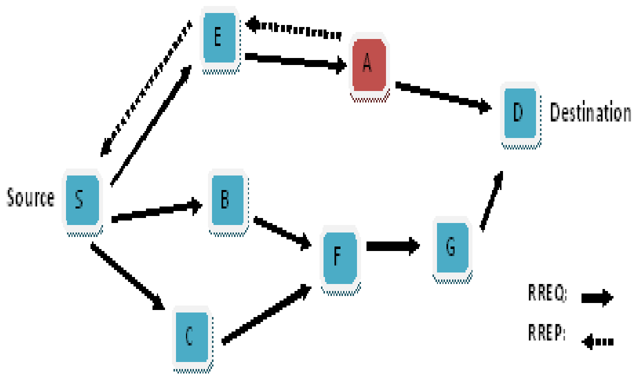

Figure 1: Blackhole Attack on AODV

The route confirmation request (CREQ) and route confirmation reply (CREP) is introduced into avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the blackhole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path. In, the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive. In another attempt, the authors analyzed the blackhole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the blackhole attack, based on differences between the destination sequence numbers of the received RREPs. The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection.

3.3 Link Spoofing Attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks. Figure 2 shows an example of the link spoofing attack in an OLSR

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

MANET. In the figure, we assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and E are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbor, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbors. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

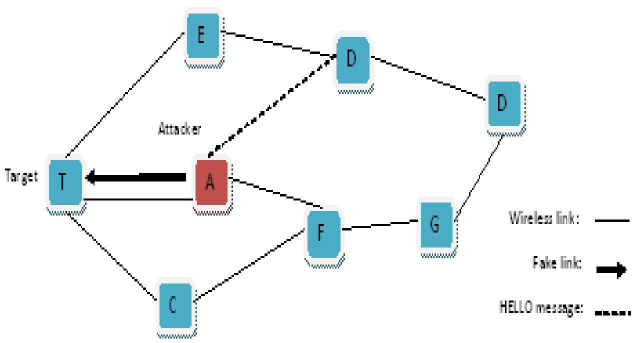

Figure 2: Link Spoofing Attack

A location information-based detection method is proposed to detect link spoofing attack by using cryptography with a GPS and a time stamp. This approach 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 equipped with a GPS. Furthermore, attackers can still advertise false information and make it hard for other nodes to detect the attack In , the authors show that a malicious node that advertises fake links with a target's two-hop neighbors can successfully make the target choose it as the only MPR. Through simulations, the authors show that link spoofing can have a devastating impact on the target node. Then, the authors present a technique to detect the link spoofing attack by adding two-hop information to a HELLO message. In particular, the proposed solution requires 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 synchronization. One limitation of this approach is that it might not detect link spoofing with nodes further away than three hops.

3.4 Wormhole Attack

A wormhole attack is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node

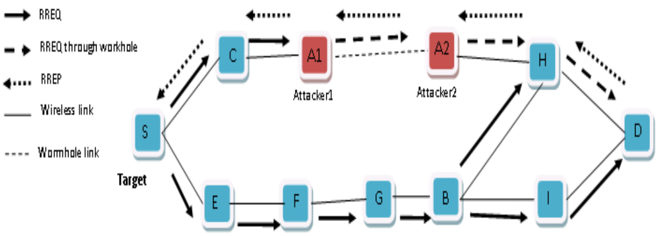

Figure 3: Wormhole Attack on Reactive Routing

D, its neighbors C and E forward the RREQ as usual. However, node A1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its colluding partner A2. Then, node A2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a highspeed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-H-D that indeed passed through A1 and A2 to send its data.

In [13], packet leashes are proposed to detect and defend against the wormhole attack. In particular, the authors proposed two types of leashes: temporal leashes and geographical Leashes. For the temporal leash approach, each node computes the packet expiration time, *te*, Based on the speed of light *c* and includes the expiration time, *te*, in its packet to prevent the Packet from traveling further than a specific distance, *L*. The receiver of the packet checks Whether or not the packet expires by comparing its current time and the *te* in the packet. The authors also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks. For the geographical leash, each node must know its own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time.

Therefore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of Geographic leashes over temporal leashes is that the time synchronization needs not to be highly tight. In, the authors offer protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of a public key infrastructure and time-stamp synchronization between all nodes that is similar to the geographic leashes. In this approach, a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum transmission range, the node judges that the HELLO message is highly suspicious and might be tunneled by a wormhole attack. In, the authors propose a statistical analysis of multipath (SAM), which is an approach to detect the wormhole attack by using multipath routing. This approach determines the attack by calculating the relative frequency of each

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

ink that appears in all of the obtained routes from one route discovery. In this solution, a link that has the highest relative frequency is Identified as the wormhole link. The advantage of this approach is that it introduces limited Overhead when applied in multipath routing. However, it might not work in a non-multipath routing protocol, such as a pure AODV protocol.

3.5 Colluding Misrelay Attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as *watchdog* and pathrater. Figure 4 shows an example of this attack. Consider the case where node A1 forwards routing packets for node T. In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

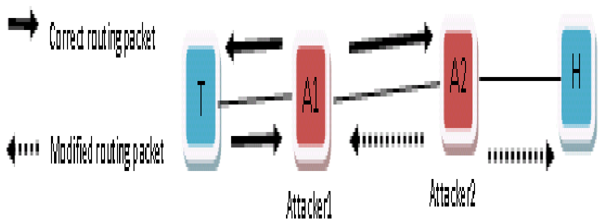

Figure 4: Colluding Misrelay Attack

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. In , the author 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 drawback of this approach is that even if we require each node to increase transmission power to be K times, we still cannot detect the attack in which K + 1 attackers work in collusion to drop packets. Therefore, further work must be done to counter against this type of attack efficiently.

4. Summary

A MANET is a promising network technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational Power, and security. Although, we have only discussed the security issues in this paper,

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

Particularly routing attacks and its existing countermeasures. The existing security solutions of wire networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. In this paper, we have discussed current routing attacks and countermeasures against MANET protocols. Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource constrained in MANET.

They still not perfect in terms of tradeoffs between effectiveness and efficiency. Some solutions work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol. Because of the characteristic of dynamic wireless network, MANET presents the following set of unique challenges to secure. Dynamic network*:* the topology of MANETs is highly dynamic as mobile nodes freely roam in network, join or leave the network on their own will, and fail occasionally. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Mobile users roaming in the network may request for anytime, anywhere security services. Resource constraints*:* the wireless channel is bandwidth constrained and shared among multiple networking entities. The computation and energy resources of a mobile node are also constrained. No clear line of defense*:* MANET has not offer a clear line of defense. Moreover, the wireless channel is accessible to both legitimate users and malicious attackers. The boundary that separate the inside network from the outside world becomes blurred. Device with weak protection: portable devices, as well as the system security information they store, are vulnerable to compromises.

Security solutions are important issues for MANET, especially for those selecting-sensitive applications, have to meet the following design goals while addressing the above challenges. Availability: ensures the survivability of the network services despite Denial of Service (DoS) attacks. A DoS attack could be launched at any layer of ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. The security service is highly available on the network layer at anytime and at anywhere. On the higher layers, an adversary could bring down high-level services. Efficiency*:* the solution should be efficient in terms of communication overhead, energy consumption and computationally affordable by a portable device. Authentication: enables a mobile node to ensure the identity of the peer node it is communicating with. Without authentication, an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Integrity: guarantees that a message being transmitted is never corrupted. A message could be corrupted because of being failures, such as radio propagation impairment, or because of malicious attacks on the network.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

Confidentiality: ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Non-repudiation: ensures that the original message cannot deny having sent the message. Nonrepudiation is useful for detection and isolation of compromised mobile nodes.

5. References

[1] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.

[2] L. R. Ford Jr. and D. R. Fulkerson, Flows in Networks, Princeton Univ. Press, 1962.

[3] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SlCON '97, Apr. 1997, pp. 197-21 1.

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

[5] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. And Networking Conf., New Orleans, LA, 2005.

[6] C. R. Dow, P. J. Lin, S. C. Chen*, J. H. Lin*, and S. F. Hwang. A Study of Recent Research Trends and Experimental Guidelines in Mobile. Ad-hoc Networks. 19th International Conference on *Advanced* Information Networking and Applications, *2005. AINA 2005, Volume: 1, On page(s): 72- 77 vol.1.*

[7] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[8] B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks," IEEE GLOBECOM '06.

[9] Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[10] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[12] Jyoti Raju and J.J. Garcia-Luna-Aceves, " A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks'," in Proceeding of IEEE ICC, June 2000.

[13] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[14] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1997.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 1, 2023. ISSN: 2348-6600
Reference ID: IJCS-457 PAGE NO: 3100-3113

[15] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

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

[17] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. lNFOCOM '97, Apr. 1997.

[18] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Com- mun. Rev., Oct. 1994, pp. 234-44.

[19] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[20] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[21] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," IEEE Wireless Commun. And Networking Conf. '05.

[22] D. Raffo et al., "Securing OLSR Using Node Locations," Proc. 2005 Euro. Wireless, Nicosia, Cyprus, Apr. 10–13, 2005.

[23] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 2002 IEEE Int'l. Conf. Network Protocols, Nov. 2002.

[24] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Publications, 2002.

[25] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.

[26] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

