Chapter

Combating Against Security Attacks against Mobile Ad hoc Networks (MANETs)

Z. M. Fadlullah

T. Taleb

M. Schöller

Abstract

Both the reactive and proactive routing protocols designed for Mobile Ad-hoc Networks (MANETS) depend on cooperation between the mobile nodes owing to the lack of a centralized administrative entity. Such a design leads to a naive assumption that all the participating nodes in a MANET are trustworthy and well-behaved. A rouge node can, indeed, manipulate this assumption and mount attacks against the concerned routing protocol to disrupt routing operations. In addition, a malicious node may also launch Denial of Service (DoS) attacks to deprive legitimate nodes from being serviced. In this chapter, we provide an insight into the various routing attacks available in literature, namely, flooding/resource consumption, wormhole, blackhole, link withholding, link spoofing, and replay attacks. We also present the possible countermeasures for thwarting these attacks. In addition, the chapter includes two case studies focusing on a uniquely crafted collusion attack against Optimized Link State Routing (OLSR) mechanism and a novel solution towards combating against wormhole attacks, respectively. The chapter concludes by presenting future research directions and final caveats concerning open issues and the more sophisticated threats against MANETs.
1. Introduction

Security is a key service for both wired and wireless network communications. In particular, the evolution in the variety and applications of ad hoc wireless networks has vastly increased the urgency to identify security threats and countermeasures to thwart these threats. Indeed, the success of ad hoc frameworks such as Mobile Ad hoc NETworks (MANETs) relies heavily on the confidence regarding security shown by the relevant users. A MANET is an infrastructure-less network, which is formed by a group of mobile nodes with wireless network interfaces. The mobile hosts dynamically establish paths among one another in order to communicate. In addition to one hop away communication, a mobile node in MANET may also function as a router to relay or forward packets, from a source node to a destination node, over multiple hops. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes. Such dynamism of MANET-based architectures lead to some inherent weaknesses and a wide variety of attacks exist that target these weaknesses. For instance, by not following the exact specifications of the considered routing protocol in MANET, a malicious node can mount routing attacks to disrupt the routing discovery phase whereby other nodes may not be able to establish a communication-path among themselves. While some attacks may target some specific routing protocols, e.g., AODV or DSR, the more sophisticated ones such as blackhole/sinkhole, byzantine, and wormhole attacks lead to serious routing security concerns, addressing which has become one of the hottest topics in MANET research domain.

In this chapter, we explore some of the existing malicious attacks against MANETs and also the techniques to detect them. First, we provide the background that takes an overview on the taxonomy of various attacks against MANETs. Then, we predominantly focus on how the networking and transport layer attacks are carried out against MANETs and how we may deal with such attacks. We also put forward the future research directions and emphasize the need for an intrusion detection system that may be appropriated with the requirements of MANETs and other ad hoc networks, and that would be able to detect not a specific kind of attacks, but various blends of threats.

2. Background: Attack Taxonomy

Broadly speaking, the attacks against MANETs can be categorized into two classes, namely external and internal attacks. In literature, these are synonymous to outsider and insider attacks [1], respectively. While the former are mounted by nodes that do not belong to the target MANET system, the latter are
launched from compromised MANET hosts. In contrast with the external attacks, the internal ones have more serious impact on the victim system. This is due to the fact that the internal (i.e., compromised) nodes have knowledge pertaining to valuable information about the network topology and also possess adequate access privileges.

Based on the nature of attack-interaction, the attacks against MANET may be classified into active and passive attacks. The former consists in replication, modification, or removing information exchanged by other nodes. The active attacks against MANET can lead to congestion, propagation of inaccurate routing information, and possible Denial of Service (DoS) scenario whereby the intended service is prevented from functioning [2] [3] [4] [5] [6] [7]. The active attacks are usually launched by either compromised (i.e., malicious) nodes or selfish hosts [8] [5] that just drop the received packets for saving their battery resources. The normal operation of the MANET is interrupted by selfish nodes since they do not take part in the routing protocols or forward packets. On the other hand, a compromised node may exploit the routing protocol to broadcast itself as having the shortest communication-path to destination. The latter (i.e., passive attacks) comprise eavesdropping of information, traffic analysis, and traffic monitoring for building statistical profiles to have an idea about the network operations and possible vulnerability of the target MANET. The passive attacks are more difficult to detect and counter against.

A common active attack is spoofing whereby a compromised node pretends to be a legitimate host. The compromised node usually exploits the lack of authentication in the current MANET protocols [9] [10]. As a consequence of spoofing attacks, the other nodes in MANET get a wrong picture of the network topology and experience network loops or partitioning. Indeed, the lack of authentication in the routing protocols adopted by MANET also leads to fabrication attacks which generate false/erroneous routing messages [11] [12] [13].

DoS attacks, in plenty of varieties and guile, remain one of the most common yet effective threats against MANETs and other ad hoc networks. In a typical DoS attack, an attacker injects a large volume of unnecessary packets into the network in order to consume a substantial amount of network resources. As a consequence, the legitimate MANET nodes compete amongst one another for the wireless channel and network connections [14] [15]. The work in [16] identifies two variations of DoS attacks against MANETs, namely sleep deprivation and routing table overflow attacks, which attempt to deplete the target node’s scarce battery power and create routes to non-existing nodes, respectively. The latter, apart from being a DoS attack, may also be categorized as a comparatively simpler routing attack. More
sophisticated routing attacks against MANETs such as wormhole attacks [17] [18], Sybil attacks [19], and rushing attacks [20] are more difficult to detect let alone prevent. It should be noted that these attacks take place on the network layer stack. On the transport layer also, MANETs are vulnerable to attacks such as session hijacking and SYN flooding. In addition, attacks are also possible against MANETs in the lower layers. For instance, traffic analysis and monitoring (passive attack), disruption of IEEE 802.11 MAC, and so on may be carried out against MANET-based hosts on the data link layer level. In the physical layer, jamming and other passive threats like messages interceptions and eavesdropping are known to exist.

However, the focus of this chapter is on the routing attacks against MANETs. To this end, in the remainder of the chapter, we focus on various security attacks against MANETs on the network and transport layers.

3. Network layer attacks against MANETs

![Diagram of network layer attacks](image)

Fig. 1. Mechanism of a simple routing attack whereby malicious node “M” inserts itself into the MANET topology.

The network layer protocols enable the MANET nodes to be connected with one another through hop-by-hop. The intrinsic nature of the MANET routing protocols, thus, ensure the cooperative communication amongst nodes by enabling them to also act as routers or intermediary devices along the communication path of a source/victim “V” and a destination “D”. In literature, different types of
attacks against MANET routing protocols have been identified through which a malicious node “M” can absorb network traffic and place itself in between “V” and “D” as shown in Fig. 1. “M” can then effectively control the network traffic flow from “V” to “D” (and also the other way around) as it becomes a router. “M” may also divert the packets exchanged between “V” and “D” via a non-optimal or a looped path. This introduces significant end-to-end delay between “V” and “D”. In an even worse scenario, “M” may direct the packets through a non-existing link. Thus, attacks against the routing protocols in the network layer contribute to a wide range of problems such as the MANET hosts not being able to find any route to destination, face network congestion, and so forth.

In addition, some attacks target specific routing protocols. For instance, if the underlying routing mechanism in Fig. 1 is Dynamic Source Routing (DSR), then “M” may modify the source route listed in the Route Request (RREQ) and/or Route Reply (RREP) packets, e.g., by adding a new node into the route, deleting an existing one from the route, change the sequence of the nodes, and so on. On the other hand, if Ad hoc On Demand Distance Vector (AODV) is used as the routing protocol, it may happen that “M” advertises a route with a fabricated distance metric that is smaller than the real one. This effectively renders the routing updates from the other MANET nodes invalid. It should be stressed also that “M” does not necessarily perform attacks at the data forwarding phase only. “$M$” may, indeed, launch routing attacks before the routing path has been determined, i.e., during the route discovery or the route maintenance phases. These various attacks are described in the remainder of this chapter.

A. MANET Routing Discovery Phase Attacks:

Some malicious users willingly do not follow the specifications of the routing protocols used in the target MANET. These attacks usually take place during the routing discovery phase. Examples of these types of threats include routing message flooding (e.g., by exchanging an overwhelming volume of “Hello”, “RREQ”, and/or “ACK” messages), routing table overflow, routing cache poisoning, and routing loop attacks [21] [22]. Indeed, proactive routing algorithms (e.g., Destination-Sequenced Distance-Vector (DSDV) [23] and Optimized Link State Routing (OLSR) [24]) for discovering the routes in MANETs are more prone to these attacks in compared to the reactive ones such as DSR [23] and AODV [23]. The reason behind this is the fact the former attempt to discover the necessary routing information periodically and prior to the when such information are required. For instance, a malicious host may overflow a victim node’s routing table by transmitting excessive route-advertisements. To this end, the malicious user (e.g., “M” in Fig. 1) broadcasts routes which may not exist at all in the target MANET topology.
Provided that “M” is successful at creating enough non-prevailing routes, a proactive algorithm may be tricked so as not to create additional routes. The proactive routing protocols are vulnerable to routing cache poisoning attacks also whereby “M” exploits the promiscuous mode of updating the routing tables of the MANET nodes. In this case, “M” ‘poisons’ routes to a victim node “V” by broadcasting spoofed packets with source route to “V” via “M” itself. As a consequence, the adjacent nodes, which notice the packets, may add this route to their respective route-caches.

B. MANET Routing Maintenance Phase Attacks:
During the route maintenance phase, a number of control messages are exchanged amongst the participating nodes in the MANET topology. Some of the attacks are mounted during this phase which broadcast spoofed control or signaling messages (e.g., broken link error messages) that trigger reconfiguring or re-establishing the route(s) from a source to a destination. For instance, in order to address the mobility of the nodes within a MANET, routing protocols like AODV and DSR adopt mechanisms for recovering from broken routes. In such mechanisms, when the destination node and/or other nodes along the path from a source to destination move, the upstream node “U” of the broken link transmits a route error message to each of the other upstream hosts. In addition, “U” also purges this particular route to the destination. A malicious user, “M” may exploit the role of “U” to broadcast false route error messages and prevent the source node (i.e., the victim node in this case) from communicating with the destination.

C. MANET Data Forwarding Phase attacks:
A lot of attacks against MANET routing protocols exploit the information forwarding functionality of the MANET nodes in the network layer [25] [26]. These attackers, in these cases, do not disrupt the route discovery and/or maintenance phases. Rather, they willingly disrupt the forwarding of data packets as per the routing table information by a number of means. For instance, a malicious user may drop silently or replay or even modify the inbound packet contents. In addition, the time-sensitive communications may be disrupted by delaying the relaying of data packets to their respective next-hop destinations or simply by injecting and forwarding dummy packets.
Next in this chapter, we provide more details pertaining to some of the sophisticated and subtle attacks against MANET routing, and also possible countermeasures against each of these attacks. They include the wormhole, blackhole, Byzantine, rushing, resource consumption, link withholding and spoofing, and replay attacks.

3.1.1 Wormhole attack:

![Diagram of wormhole attack]

The wormhole attack, one of the most sophisticated and serious threats against MANET routing, comprises a pair of attackers. These two attackers act in collusion to record packets at a particular location in the MANET topology and replay them at another node by using a high speed private network. Fig. 2 demonstrates an example scenario of this attack where “M₁” and “M₂” are the colluding attackers, and “V” is the victim node. When “V” broadcasts a RREQ message to find a route to a node “D” (i.e., when “V” and “D” are the source and destination nodes, respectively), the immediate one-hop away neighbors of “V”, namely “A” and “F”, forward the RREQ message to their respective neighbors “B” and “M₁”. However, as “M₁” receives the RREQ from “F”, it tunnels the RREQ message to its colluding partner “M₂”. The latter then broadcasts the RREQ message to its one-hop away neighboring node “G”, through which the RREQ is delivered to the destination node, i.e., “D”. Due to the high-speed link...
chosen by the tunnel between “M₁” and “M₂”, it takes shorter time for this particular route to deliver the RREQ message to “D” in contrast with that taken over the {V-A-B-C-E-D} path. As a consequence, the route {D-G-F-V} becomes the apparent choice for “D” for issuing a unicast RREP message as a response to the RREQ received from “V”. Therefore, “D” ignores the same RREQ that arrives at a later time and thus, invalidates the legitimate route: {V-A-B-C-E-D}. This forces “V” to select the route {V-F-G-D}, which, indeed, goes through the “M₁” and “M₂”, the malicious users, which can tamper with its data packets.

3.1.2 Countermeasures against the wormhole attack:

In order to detect and combat against the wormhole attack, two types of packet leashes were introduced as an effective technique in [27], namely temporal and geographical leashes. In the former, every node in the MANET calculates the packet expiration time, tₑ and includes tₑ in its packets so that the packet may not travel further than a particular distance, L. When a packet containing this information arrives at a node, the receiver compares the current time with the value of tₑ in the packet. With such information, the destination node (e.g., D in Fig. 2), may then be able to determine, whether a RREQ was tunneled possibly over a high-speed link to serve a malicious purpose. In addition, tₑ is authenticated by the involved ends so that it may not be tampered with by malicious nodes such as M₁ and M₂. However, the temporal leash needs all the nodes in the considered MANET topology to be strictly time-synchronized with one another. On the other hand, in case of the geographical leash, every node must know two pieces of information, namely, its respective position in the MANET it belongs to and the transmission time. This enables the receiver to evaluate neighbor relations by calculating distance between itself and the original source of the packet.

Based on the location information, further solutions evolved to counter wormhole attacks. For instance, the work in [28] offers protection against wormhole attacks, specifically in MANETs that use OLSR as the routing protocol. This, however, requires an integration of the public-key infrastructure with the time-synchronization between all the nodes. In this scheme, every node, while issuing a HELLO message, inserts its current position and also the current time stamp in the HELLO message. A node that receives a HELLO packet from one of its neighbors can then use the information embedded in the packet to compute the distance between itself and the neighbor. In case the computed distance exceeds the maximum transmission range, the HELLO message is considered to be highly suspicious (i.e., possibly tunneled over a wormhole attack). Interested readers may also refer to additional mechanisms in
literature (e.g., SECTOR [29] and directional antenna based detection of wormhole attacks [30]) without the need of clock synchronization amongst the MANET nodes.

Statistical analysis has also been adopted in literature to detect wormhole attacks. For example, Qian et al. [31] introduced a statistical analysis over multiple path routing. This scheme computes the relative frequency of every link that is found in all the obtained routes during a single route discovery. The highest relative frequency is then identified as the wormhole link. While this scheme has low overheads when applied in multipath routing, it does not work well with non-multipath routing protocols such as AODV.

A potential solution to thwart wormhole attacks is to integrate intrusion detection and/or prevention systems in the MANETs. Other countermeasures have considered, in addition to software-based intrusion detection systems, designing specific hardware and signal processing techniques. The hypothesis behind such solutions suggests that if the data bits transmitted over some special modulating scheme is known only to the neighboring nodes, they cannot be affected by closed wormholes.

3.2.1 Blackhole attack:

In case of the blackhole attack as shown in Fig. 3, a malicious node “M” claims to possess an optimum route from a given source, “V” to a destination, “D”, and transmits this forged routing information to the other MANET nodes. As a result, the other users are tricked to forward their data packets through the malicious node. For instance, if the target MANET uses AODV as the routing protocol, “M” may generate
a false RREP consisting of a non-existing destination sequence number, which is equal or higher than that in the RREQ from the victim node (i.e., the source node “V”). This implies that the malicious node “M” claims that it possesses a sufficiently fresh route to the destination. This prompts “V” to choose this particular route (i.e., V-A-B-M) for sending data packets through the attacker. Consequently, “M” may willingly delay/drop the data packets or change the contents of the packets. However, “M” runs the risk that its neighboring nodes, e.g., “B” and/or “F” may monitor and expose the ongoing attacks. To avoid such detection, “M” may execute more sophisticated versions of the blackhole attack whereby packets are intercepted and rather than dropping every data packet, the intercepted packets are forwarded selectively. Indeed, when “M” makes modifications only to those packets arriving from “V” but not to the ones arriving from “B” or “F”, it reduces the chance of detecting this malicious activity by the neighboring nodes.

3.2.2 Countermeasures against the blackhole attack:

In order to defend against possible blackhole attacks, security-aware ad hoc routing protocol or SAR was designed [32] which is based upon conventional on-demand MANET routing protocols such as AODV and DSR. SAR employs two techniques as follows. First, a security metric is inserted in the RREQ packet. For achieving a decent trust level (e.g., for avoiding identity theft or identity spoofing), SAR uses a simple shared secret to generate a symmetric cryptographic key per trust level using which the packets are encrypted. In other words, a node which belongs to a different trust level is unable to read the encrypted RREQ or RREP packets. Second, an alternate route discovery mechanism is used. When the other nodes along a route receive the RREQ packets from a particular source, they verify the trust level associated with the security metric information embedded in the packets. Given that the trust level is satisfied, an intermediary node would start processing the packet (i.e., forward it to the next node along the route). If the trust level is not within a pre-specified satisfaction level, the intermediary node drops the packet. When the destination node is satisfied with the security attributes or trust levels associated with the overall end-to-end path from the source to destination nodes, it generates a RREP packet with the specific security metric. Otherwise, it notifies the source node that the communication cannot be continued via this route (as it may be already compromised) and thus permits the sender to adjust its security level for finding an alternate route. Indeed, there are chances that a malicious node changes the
security metric to a higher or lower level and disrupt the flow of packets. This remains a shortcoming of the SAR approach.

Among other approaches to combat against blackhole attacks, the work in [33] introduces in the routing protocols the use route confirmation request and response, denoted by CREQ and CREP, respectively. In this work, each intermediary node, in addition to sending RREP, sends a CREQ message to its next-hop neighbor towards the destination node’s direction. After receiving the CREQ, the next-hop node searches, in its cache, for a route to the destination. If such a route to the destination is, indeed, available, the next-hop node transmits CREP message to the source. The source, after receiving this CREP message, checks whether the path in the RREP message is the same as that in the CREP one. If so, it deems the routing information to be correct. However, this approach is not sufficient to counter against a pair of nodes working in collusion that attempt to perform blackhole attacks. Because, when the next-hop node is also colluding, it can generate and send forged CREPs containing inaccurate routes. To overcome this issue of colluding nodes, Al-Shurman et al. [34] devised a mechanism which makes the source node wait for RREP messages arriving from more than two nodes. From multiple RREPs, the source node can then evaluate the accuracy pertaining to the path information. This particular approach is also not without its shortcomings, the obvious being the added latency during which the source node must wait for multiple RREP packets to arrive.

A different approach consists in not merely circumventing the blackhole attacks but also detecting them. This approach was inspired by the analysis conducted by Kurosawa et al. [35] that reveals that a malicious user must increase the destination sequence number to such an extent as to convince the source node that the provided path is optimum enough. Following this analysis, a statistical detection scheme was envisioned to discover the anomalies, i.e., the increasing differences between the destination sequence numbers of the received RREPs, which would suggest possible blackhole attacks. While such anomaly-based intrusion detection approaches do not produce additional routing traffic or require any modification in the existing routing protocol, they may often be susceptible to high number of false positives and thus disrupt communications.

3.3.1 Byzantine attack:

A byzantine attack comprises either a single compromised nodes or a group of compromised/colluding nodes in between the route from the source end to the destination node. The compromised node(s)
target the MANET by mounting attacks such as creating routing loops and directing data packets via non-optimal paths which lead to degradation or disruption of the routing services [36].

3.3.2 Byzantine Attack Prevention:

Cr´epeau et al. [37] introduced Robust Source Routing (RSR), a secure MANET on-demand routing protocol, capable of delivering packets to their respective destinations even in Byzantine attack-like adversarial conditions. RSR, by using Fore-Runner (FR) packets, notify the intermediate nodes along a route that they are to expect the specified data flows within given time frames. If an intermediate node has not received any data flow within the expected time, it informs the source node about this event. By this way, the links with selfish and/or active malicious nodes can be identified and isolated.

3.4.1 Rushing attack

In [20], the authors introduced a new form of routing attack called the rushing attack, which acts as an effective DoS type threat against all conventional on-demand MANET routing protocols. In fact, even the secure routing protocols (e.g., SAODV and AODV secured with SUCV) were shown to be vulnerable to this particular rushing attack.

Fig. 4. A MANET topology where “M” may performs rushing attacks [20].
In case of a typical on-demand ad hoc routing protocol, a node that intends to discover a route to a given destination floods the target network with RREQ packets. In order to keep the impact of the flood as minimal as possible, the nodes in conventional routing protocols only forward the request that arrives first from each Route Discovery. This particular mode of route discovery operation is exploited by the rushing attack. For instance, in case of DSR route discovery, let us refer to Fig. 4, where “S” and “D” refer to the source and destination nodes, respectively, “M” denotes the rushing attack-node, and “G” and “H” are the one-hop neighbors of “D”. If the RREQs for this discovery forwarded by “M” are the first ones to reach “G” and “H” (this is possible in a number of ways as investigated in [20]), then any route discovered by this route discovery operation will include a hop through “M”. Simply put, when a neighbor of the target “D”, i.e., “G” or “H”, receives the rushed RREQ from the attacker, it forwards that request alone, and does not forward any further RREQ from this route discovery. Even if non-attacking RREQs from “S” reach “G” and “H” at a later time, those legitimate requests are discarded. As a consequence, “S” fails to discover any useable route or safe route without the involvement of the attacker.

3.4.2 Rushing Attack Solution:

The authors in [20] proposed Route Discovery Protocol (RAP), which replaces the standard mechanism of the conventional ad hoc routing protocols that are inherently vulnerable to rushing attacks. In fact, RAP combines three techniques to prevent the rushing attack, namely a secure neighbor discovery mechanism, a secure route delegation acceptance protocol, and the randomized selection of the route request that will be forwarded.

3.5.1 Resource consumption attack:

The resource consumption or sleep deprivation attack consists in an attacker or a compromised node to consume the resources of the victim node or the target MANET [38]. For example, the aim of the flooding attack is to exhaust resources such as the network bandwidth by forwarding excessive packets to victim nodes, or the computational power and battery life of a victim node by requesting unnecessary route discovery in an excessive volume. A simple example consists of an adversary node targeting AODV routing protocol by transmitting a large number of RREQ packets in a short period of time to a non-existing destination node. Since no node will respond to these RREQs, these packets will simply flood the MANET, and consume the network bandwidth and deplete the scarce battery power at of the nodes.
Furthermore, the work in [39] demonstrates that such a flooding attack can degrade the overall MANET throughput by 84%.

### 3.5.2 Resource consumption attack Prevention:

Yi et al. [38] envisaged a simple yet effective mechanism to prevent the resource consumption attacks, particularly in MANETs that use AODV as the routing protocol. In this mechanism, every node monitors and computes the respective RREQ rates of its neighbors. If the RREQ rate of a neighbor is found to exceed a threshold defined *a priori*, the node blacklists the neighbor and drops further RREQs from that particular neighbor. The main problem of this mechanism is that it is prone to false positives, and may end up blacklisting legitimate nodes. The work in [39], on the other hand, uses a similar anomaly-based detection mechanism which, instead of using a fixed threshold, learns from the statistical analysis of different rates of RREQ packets and computes the threshold on the fly.

### 3.6 Link Withholding and Link Spoofing Attacks:

The names of these attacks are somewhat self-explanatory. In case of a link withholding attack, a malicious node willingly withholds or ignores the requirement to advertise the route to a specific node or a collection of nodes. As a result, other hosts are unable to find links to communicate with those nodes. In link withholding attack launched against Topology Control (TC) messages in OLSR, Kannhavong et al. [40] show that a malicious node can isolate a particular node and prevent it from communicating with other nodes in the MANET. Their proposed detection technique works on the hypothesis that if a node receives only a HELLO message from its Multipoint Distribution Relay (MPR), but does not receive any TC message from the MPR, the node evaluates the MPR to be suspicious. The node then switches to another MPR. This approach, however, fails to detect attacks launched by two malicious partners that lie next to one another whereby the first malicious node pretends to advertise a TC message while the second one discards that TC packet.

On the other hand, in link spoofing attacks, a malicious node advertises forged routes. For instance, an attacker may broadcast a spoofed link with the victim’s two-hop away neighbors in an OLSR-based MANET. As a result, the victim chooses the malicious node as its MPR. As MPR, the malicious node can discard the TC messages and other routing traffic from the victim, or modify the data packets arriving from the victim intended for a different destination.
For detecting a link spoofing attack, the work in [41] envisioned a detection scheme which relies on spatial information obtained from GPS and a time-stamp that are encrypted. Each node, in this scheme, advertises to other nodes its GPS coordinates and the time-stamp. Thus, it becomes possible to detect possible link spoofing cases by computing the inter-nodal distances of two given nodes and to also check whether they lie within the maximum transmission range or not. The main problem pertaining to this solution is that every node requires being equipped with GPS which may not be always possible. Our first case study, provided later in this chapter, will focus on a uniquely crafted scenario for link withholding/spoofing with hints of how to solve such problems.

3.7 Replay Attacks

The topology of a MANET frequently changes because of the mobility of its nodes. This dynamic change in the MANET topology means that the current network topology may not prevail even after a few seconds. In replay attacks [42], the malicious nodes record the legitimate control messages (e.g., TC messages in case of OLSR) of other nodes and retransmit them at a later time. As a result, the routing tables of the MANET nodes are updated with old and stale routes. By this way, replay attacks may be exploited for impersonating a particular node or simply disrupting the routing operations of the target MANET.

In order to protect MANETs from replay attacks, the work in [42] employs a solution based on time-stamps and asymmetric encryption. The solution simply compares the current time with the time stamp embedded in the received control messages from other nodes. If the time stamp in a received control packet deviates much from the current time, the receiving node considers it to be a possible replay attack and therefore, the packet is discarded to avoid updating the routing table with stale information. However, this solution still remains vulnerable to wormhole attacks comprising a pair of colluding attackers that employ a high-speed network for replaying messages in a far-away location with rather low latency.
4. Transport Layer Attacks against MANET

Transport layer protocols such as TCP (Transport Control Protocol) are used in MANET for establishing end-to-end connections amongst MANET nodes and ensure reliable packets delivery over the end-to-end connections. In addition, similar to the wired communications, flow and congestion control is also possible in MANET by adopting TCP-like transport protocols. However, due to the intrinsic weakness of TCP, SYN flooding or session hijacking attacks are possible also in the MANET environment. Furthermore, MANETs are attributed with typically higher channel error rates in contrast with their wired counterparts. This augments to TCP-related problems because TCP is unable to differentiate the nature of the loss (e.g., whether the loss is owing to congestion, random error, channel error, or malicious attacks) and as a result, it multiplicatively decreases its congestion window. This eventually affects the performance of the MANET [43] substantially. In the remainder of this section, we take a brief overview of the SYN flooding and session hijacking attacks against MANETs.

4.1 SYN flooding attack:

For two MANET nodes to establish a TCP connection, they need to perform a 3-way handshake as shown in Fig. 5. In the first step, the source node “S” needs to initiate the connection with the destination node “D” by sending a SYN packet along with a sequence number “P”. As a response to this, “D” then transmits to “S” a SYN/ACK message including its own sequence number “Q” and the acknowledgment number “P+1”. In the final step, “S” issues an “ACK” message (with ack. number “Q+1”) to “D”. Thus, “S” and “D” establishes a TCP connection. In case of SYN flooding attack, “S” initiates a large number of TCP
connections with the victim node “D”. However, “S” spoofs the return address of the SYN packets and thus does not complete the step 3 of these TCP connections (i.e., they are left open in mid-way). “D”, upon receiving the SYN packet from the attacker (“S” in this case), issues immediately the SYN-ACK packets to the spoofed address, which often does not exist in the MANET. As a consequence, “D” awaits reception of ACK packets (in step 3 of the TCP handshake). A large number of these half-opened connections may then overflow the buffer maintained by “D”. Such a buffer overflow results in “D” not being able to accept any legitimate request for establishing TCP connection from other MANET nodes. Although a half-open connection normally should expire within a timeout period, the attacker can exploit this by transmitting SYN packets with spoofed addresses at a rate faster than this time-out value.

4.2 Session hijacking attack:

![Diagram of TCP ACK storm steps]

The attacker in a session hijacking scenario exploits the unprotected session following to its initial setup. The attacker forges the IP address of the victim node, computes the sequence number expected by the target, and then launches a DoS attack against the victim. By so doing, the attacker pretends to impersonate the victim node and maintain communicating with the target over the already established TCP session. An example of the session hijacking attack is the TCP ACK storm problem as depicted in Fig. 6. Here, nodes “N1” and “N2” have established a TCP connection. An attacker “M” spoofs the IP address...
of “N2” and injects data into the session of node “N1”. Then, “N1” acknowledges the receipt of this information by transmitting an ACK packet to node “N2”. As “N2” notices a different sequence number in the received ACK packet from “N1”, it reissues its last ACK packet to “N1” in order to resynchronize the TCP session. This repeats over and over, leading to an ACK storm. Indeed, it is even easier to hijack sessions in a similar way with connection-less transport protocols such as UDP.

5. Case Studies

In this section, we provide two case studies that address attacks on the OLSR protocol. OLSR is a table driven proactive routing protocol that periodically exchanges messages amongst the nodes in order to maintain the accurate topological information of the considered MANET. Each node can compute the optimal route to a given destination based upon the topological information. By employing multipoint relays (MPR), the OLSR protocol is able to immediately provide optimal routes. Each node chooses a set of its neighbor nodes as MPRs, which are responsible for generating and forwarding the topology information all over the MANET. In the first case study, a collusion attack is presented in which two or more attackers collaborate among one another to launch a routing attack [44]. In the second case study, an effective method is presented for detecting and preventing worm hole attacks against MANETs using OLSR as the routing protocol [45].

5.1 A Collusion Attack Against OLSR-based MANETs

The collusion attack demonstrated in [44] is shown in Fig. 7. In the considered MANET topology depicted in the figure, there are two malicious nodes, namely “M1” and “M2”. The victim node is denoted by “V”. “M1” sends HELLO message including the address list of the two-hop neighbors of “V”. As per the OLSR protocol, “V” then selects “M1” to be its only MPR. Then “M1” selects “M2” as its only MPR. As a consequence, the TC messages generated by “V” are forwarded only via “M1”. In addition, “M1” drops the TC message from being forwarded to “B” and “F”. Also “M2” discards the TC message and it is not forwarded to node “F”. This collusion attack means that the TC messages from the Victim “V” are not relayed via “M1” and “M2” to the remaining nodes (e.g., I, J, F, H, and so on). Therefore, the remaining nodes are unable to construct routes to the victim node “V”.

18
This specific collusion attack may be detected if every node in the considered MANET topology is able to learn the topology setting up to more than two hops. The detection scheme provided by Kannhavong et al. [44] adds in the HELLO message of every node its two-hop neighbors list. This is done to verify if the link information advertised by the one-hop away neighbors are accurate. In case that a node discovers that any of its one-hop neighbors has provided inconsistent routing information, it identifies that neighbor as a malicious one and avoids it.

5.2 Detecting wormhole attacks against OLSR protocols

Naït-Abdesselam et al. [45] envisioned a unique method for detecting and preventing wormhole attacks against OLSR-based MANETs. Their approach consists of a number of steps, namely detecting suspicious links and wormhole verification.

In the first step, the nodes in the MANET attempt to detect links suspected to be part of a wormhole. To this end, every node periodically advertises a HELLO message so that it may discover its own one-hop neighbors. When another node receives this HELLO message, it deems the originator of the message to be its actual neighbor. The wormhole attack, however, may also contribute to such a HELLO message,
which is not necessarily originated from just one hop away from the receiving node. To detect such
suspicious links, Naït-Abdesselam et al. define two novel control packets for the OLSR protocol, namely
HELLO$_{req}$ and HELLO$_{rep}$. The former is an extension to the original HELLO message used in the
conventional OLSR protocol and it can be configured with either of the following two options: (i) it may
function as the original message by default, or (ii) it can be used by its originator to request an explicit
response from its neighbors. In the second operational mode, the neighbors then respond by issuing
HELLO$_{rep}$ to the querying node. The message types of the conventional HELLO, HELLO$_{req}$ and HELLO$_{req}$
are differentiated by employing two unused bits in the original message.

Following each $N$ standard HELLO message transmissions, a MANET node has to transmit a HELLO$_{req}$
message. Here, $N$ reflects the desired security level, i.e., if an application requires a high security level
and is willing to detect the attackers rapidly, $N$ should be adjusted to a relatively small value. According
to the above mentioned definition of HELLO$_{req}$, this prompts explicit HELLO replies from its neighboring
nodes. The originating node waits for the HELLO$_{rep}$ message from its neighbors up to a pre-specified
time-out value. On the other hand, when a node receives a HELLO$_{req}$ packet, it records the address of
the sender and the time left until it is scheduled to send its next HELLO message, denoted by $i$ and $\Delta_i$,
respectively. In OLSR, the default value of HELLO message transmission interval is two. If a receiver is
queried by multiple sources, it delays the corresponding replies until it is scheduled to send its normal
HELLO message. In addition, it piggybacks the responses to this HELLO message. This is done in order to
avoid flooding the MANET with an excessive number of HELLO replies. Then, for each piggybacked
response, the node attaches the recorded address of the sender of the respective HELLO$_{req}$ and the $\Delta_i$
values.

Upon receiving a HELLO$_{rep}$ packet, a node needs to verify if the received packet contains information
pertaining to any of its pending requests made earlier. If the received HELLO$_{rep}$ has no such information,
it is treated as an ordinary HELLO message. Otherwise, the node evaluates if the HELLO$_{rep}$ message came
within the scheduled timeout interval. If so, the node considers the route between itself and the node,
which issued the HELLO$_{rep}$ message, to be safe. Therefore, it (i.e., the originator of the HELLO$_{req}$ message)
adds the responding node as its neighbor. On the other hand, if the HELLO$_{rep}$ is received by the
originator after the expiration of its scheduled timeout value, the originator deems the link between
itself and the responder to be suspicious. As a consequence, the originator stops communicating with
the suspected node until the wormhole verification process is completed.
The wormhole verification process commences following the detection of suspicious links. This is carried out by the originator of the HELLO$_{req}$ message. The objective of this procedure is to verify if there exists any wormhole tunnel along the route comprising the originator and the other end of the suspicious link. Two more novel messages are annexed in the OLSR protocol for this purpose, namely a probing packet and an acknowledgment to the probing packet, denoted by ACK$_{prob}$. The originator node transmits a probing packet to each of the suspected nodes. As a response to the probing packet, the other nodes respond to the originator by sending ACK$_{prob}$ packets. For example, a node “A” queries a suspicious node “B” about its wormhole status reputation. “B” responds with an ACK$_{prob}$ message which also contains its own opinion about the wormhole status reputation of node “A”. In addition, ACK$_{prob}$ packets also contain the processing time information so that an accurate timeout value can be adjusted. For secure exchange of these messages, the transmission of probing and ACK$_{prob}$ packets are encrypted and authenticated. To conclude if a suspicious link is, indeed, traversing a wormhole tunnel, the originator node compares its evaluation of the reputation of the other endpoint of the suspicious link with the remote node’s evaluation of its own reputation status. Experimental results demonstrate that the detection accuracy under this approach depends on the correlation between the number of MANET nodes and the wormhole tunnel length. For example, in a small scale MANET with 15 nodes, the detection accuracy remains over 95% with increasing values of the tunnel length. On the other hand, for larger MANET topologies with 30 up to 50 nodes, the detection accuracy decreases significantly as the tunnel length increases. This is attributed to the fact that if the number of neighboring nodes increases, the malicious nodes are more likely to exploit more neighbors to form longer wormhole tunnels even though the neighboring nodes are far away from one another. The results also suggest that in OLSR, every node periodically dispatches routing control messages. This increases the overheads in large-scale networks because the traffic increases substantially when these routing control messages are passed through the wormhole tunnels.

6. Open issues and Future Directions of Research

Security is, indeed, a crucial issue in determining the success and wide use of MANET-based applications. As described in the earlier sections, a lot of security threats and vulnerabilities in MANET already exist in literature. Future research should also be focused on reducing the design and deployment cost of the security provisioning so that they would be more suitable for MANET and other
ad hoc wireless environments such as vehicular networks and wireless sensor networks. In addition, most of the conventional security mechanisms attempt to single out the known threats and deal with them individually. In other words, the countermeasures to a particular type of threat (e.g., the blackhole attack) may not necessarily be sufficient enough to thwart other types of attacks. Therefore, it is important for future researches in this domain to pay more attention towards countering against novel/unknown attacks. Furthermore, in case of cross-layer attacks, the security mechanisms need to be enforced on each layer separately which is cumbersome. This is worth exploring in future to make MANETs more secure and reliable.

By definition, MANETs are self-organized and they are not bound by any infrastructure and/or central authority. This leads to a plethora of open research challenges including self-organized key management, cooperation incentives, authentication and access control, context-awareness and quality of security services, and so forth. There is also a research scope for integrating security primitives in MANET-based systems. For instance, key management protocols may help enhance the overall security level of a MANET as perceived by its users. Indeed, substantial research may be carried out on designing robust key management systems, trust-based routing protocols, and integrating authentication and encryption in different layers. The major research directions are summarized as follows.

6.1 Intrusion Detection and Prevention:

In contrast to other wired and wireless networks, MANETs have unique features such as open nature, mobility of the nodes, and dynamic change in the topology. As a result, the conventional intrusion detection and prevention methods from security attacks may not be applicable to MANETs. The intrusion detection theme is of significant importance in discovering a potential attack before it may severely impact the target network and the victim(s). In a nutshell, the intrusion detection techniques that have been so long adopted in older wireless networks are not directly suitable for MANET environments. The future intrusion detection systems for MANETs and other ad hoc networks need to be both distributed and cooperative whereby each node should participate in the intrusion detection. That is, the intrusion detection is performed locally at every node and also on a more wide scale where the neighboring nodes share the intrusion detection information and collaborate with one another to trace suspicious links. The second case study in Section 5.2 indicates that researches have already started towards this direction.
Furthermore, upon detecting an intrusion or attack, the adequate response is also required. Intrusion prevention and/or response systems are to evolve to protect MANETs in future so that a wide range of responses may be adopted. The response may involve resetting the communications channels among the nodes, tracing back the compromised nodes and excluding them from the MANET, and so forth. In fact, most of the contemporary work on intrusion preventive and response methods are considered to be the second line of defense. Constructing a reliable trust-based framework for MANET and integrating it with the current preventive methods may be possible in future research work.

6.2 Cryptographic techniques

Cryptographic operations such as encryption and decryption of data packets and control information need to be used wherever applicable to strengthen MANET security. This requires adequate key management schemes. The public key cryptography schemes often depend upon the centralized Certificate Authority (CA) entities, and the centralization issue is rather in contrary to the design and functional goals of MANETs. In fact, a number of researches have investigated whether several MANET nodes may be distributed to act as CAs based on a secret sharing mechanism. However, the mobility of the nodes makes it more difficult to obtain a dynamic reconfiguration of the CAs in MANETs and this issue remains yet to be resolved. Researchers should also decide whether to adopt more efficient distributed trust models such as PGP or employ the simple yet computation-efficient symmetric cryptography for the sake of saving the scarce battery resources of the ad hoc wireless nodes. The tradeoff issue pertaining to the level of security and efficiency is definitely going to be an issue in MANET security provisioning.

6.3 Resiliency

Due to the fact that many of the attacks against MANETs are unpredictable, a resiliency-oriented security solution is required to be developed in future. This will help the legitimate nodes to recover from a possible network failure as soon as possible. While cryptographic solutions in Section 6.2 only offer a subset of solutions, the multi-faceted solutions towards a resilient MANET architecture is expected to evolve in future.

7. Conclusions

In recent time, mobile ad hoc networks have emerged as a promising technology and gained tremendous attention from researchers. Since these networks can be rapidly deployed without the need
of any pre-defined infrastructure, they can be easily applied to various scenarios ranging from emergency operations and disaster relief to military services, vehicular networks, and other sensitive domains. However, their lack of infrastructure and/or central authoritative environment offers plenty of opportunities to malicious nodes for launching a wide array of attacks. Therefore, in order protect the sensitive information, which are exchanged in MANETs, security provisioning is of utmost importance.

One of the main research challenges in MANET security provisioning is that these networks are already resource-constrained. For instance, a MANET has scarce battery power, computational/processing ability, and also limited bandwidth. As a consequence, the conventional security schemes for wired and other wireless networks may not be directly applicable to MANETs. This particular issue also makes MANETs much more susceptible to security attacks.

This chapter reviewed the current state of-the-art transport layer and routing attacks. In particular, the counter-measures to circumvent the routing attacks along with their pros and cons have also been delineated. This chapter reveals that while a large body of literature is available in countering many security attacks against MANETs, they usually focus on dealing with only one type of attack. Therefore, we are still far from achieving a perfect solution that may integrate all existing security solutions effectively.

References


**Keywords:**

Mobile Ad hoc networks (MANETs), security attacks, routing attacks, OLSR, blackhole attack, wormhole attack, rushing attack, intrusion detection.
Questions and Answers

Q 1. What is the difference between external and insider attacks?

The attacks against MANETs may be classified into two broad groups: external (outsider) and internal (insider) attacks. In case of an external attack, the attack-node does not belong to the target MANET. On the other hand, insider attacks feature compromised MANET hosts that turn out to be attackers. The internal (i.e., compromised) nodes have knowledge pertaining to valuable information about the network topology and also possess adequate access privileges. As a consequence, the internal attacks have a more serious impact on the victim system.

Q2. What are selfish nodes in a MANET and how do they lead to security vulnerabilities?

Selfish hosts in a MANET just willingly drop the received packets for saving their own battery resources. The normal operation of the MANET is interrupted by selfish nodes since they do not take part in the routing protocols or forward packets. This leads to incomplete information of the route from a source to destination via the selfish nodes.

Q3. In how many ways is it possible to target a MANET on the network layer?

The network layer attacks against MANETs can be launched in three ways. The first variety of networking attacks target the routing discovery phase. The second type of attack is launched during the MANET routing maintenance phase. There are also networking attacks during the data forwarding phase.

Q4. What is the wormhole attack?

The wormhole attack is considered to be one of the most serious threats against MANETs routing. It consists of two malicious users in collusion. A high-speed private network connects these two attackers. The first malicious node collects packets at a certain point in the MANET topology and replays them at the other node by using the high-speed network. Thus, the packets intended to a particular destination node are dropped.

Q5. What are the differences between wormhole and byzantine attacks?

In traditional wormhole attacks, the attacker may trick two non-malicious nodes to assume that there exists a direct link between them. On the other hand, in case of a Byzantine attack, the
wormhole link exists between the compromised nodes and not between the non-malicious ones. This implies that these end nodes cannot be trusted to follow the routing protocol.

**Q6. What makes the rushing attacks so dangerous?**

Usually the attacks against MANET target a particular routing protocol (e.g., AODV, OLSR, and so forth). The rushing attack, on the other hand, acts as an effective DoS type threat against all conventional on-demand MANET routing protocols. In fact, even the secure routing protocols (e.g., SAODV and AODV secured with SUCV) were shown to be vulnerable to this particular rushing attack.

**Q7. How can we prevent rushing attacks?**

The Route Discovery Protocol (RAP), which replaces the standard mechanism of the conventional ad hoc routing protocols that are inherently vulnerable to rushing attacks, is used to thwart rushing attacks. RAP combines three techniques to prevent the rushing attack, namely a secure neighbor discovery mechanism, a secure route delegation acceptance protocol, and the randomized selection of the route request that will be forwarded.

**Q8. Which technique is used to protect MANETs from replay attacks? Is it full-proof?**

The scheme in [42] employs a solution based on time-stamps and asymmetric encryption. This scheme simply compares the current time with the time stamp embedded in the received control messages from other nodes. If the time stamp in a received control packet deviates much from the current time, the receiving node considers it to be a possible replay attack and therefore, the packet is discarded to avoid updating the routing table with stale information. However, this solution is not full-proof as it still remains vulnerable to wormhole attacks comprising a pair of colluding attackers that employ a high-speed network for replaying messages in a far-away location with rather low latency.

**Q9. What is the implication of multi-layer attacks against MANETs?**

Usually, the individual attacks against MANETs target one of the layers. More sophisticated attacks are expected to evolve to target various layers at the same time. In case of such cross-
layer attacks, the security mechanisms need to be enforced on each layer separately which is, indeed, cumbersome.

**Q10. What is the prospect of using key management schemes in enforcing security in MANETs?**

There is a research scope for integrating security primitives in MANET-based systems. For example, key management protocols may assist in enhancing the overall security level of a MANET as perceived by its users. Indeed, substantial research may be carried out on designing robust key management systems, trust-based routing protocols, and integrating authentication and encryption in different layers.

**Q11. Can conventional intrusion detection schemes be used in MANETs?**

In contrast to other wired and wireless networks, MANETs have unique features such as open nature, mobility of the nodes, and dynamic change in the topology. Consequently, the conventional intrusion detection and prevention methods from security attacks may not be directly applicable to MANETs. The intrusion detection theme is of significant importance in discovering a potential attack before it may severely impact the target network and the victim(s).
Biography

Z. M. Fadlullah received his M.S. degree from the Graduate School of Information Sciences (GSIS) at Tohoku University in March, 2008. He obtained his Bachelor degree in Computer Science and Information Technology from Islamic University of Technology (IUT) in 2003. Currently, he is working toward a PhD degree at GSIS, Tohoku University. His research interests are in the areas of network security, specifically intrusion detection/prevention, trace-back mechanisms, and Quality of Protection.

Tarik Taleb is currently working as Senior Researcher at NEC Europe Ltd, Heidelberg, Germany. Prior to his current position and till Mar. 2009, he worked as assistant professor at the Graduate School of Information Sciences, Tohoku University, Japan. From Oct. 2005 till Mar. 2006, he was working as research fellow with the Intelligent Cosmos Research Institute, Sendai, Japan. He received his B. E degree in Information Engineering with distinction, MSc and PhD degrees in Information Sciences from GSIS, Tohoku Univ., in 2001, 2003, and 2005, respectively. His research interests lie in the field of architectural enhancements to 3GPP networks (i.e., LTE), mobile multimedia streaming, wireless networking, inter-vehicular communications, satellite and space communications, congestion control protocols, network management, handoff and mobility management, and network security. His recent research has also focused on on-demand media transmission in multicast environments.

Dr. Taleb is on the editorial board of the IEEE Transactions on Vehicular Technology, IEEE Wireless Communications, IEEE Communications Surveys & Tutorials, and a number of Wiley journals. He also serves as Vice Chair of the Satellite and Space Communications Technical Committee of the IEEE Communication Society (ComSoc) (2006 - present). He has been on the technical program committee of different IEEE conferences, including Globecom, ICC, and WCNC, and chaired some of their symposia. He is the recipient of the 2009 IEEE ComSoc Asia-Pacific Young Researcher award (Jun. 2009), the 2008 TELECOM System Technology Award from the Telecommunications Advancement Foundation (Mar. 2008), the 2007 Funai Foundation Science Promotion Award (Apr. 2007), the 2006 IEEE Computer Society Japan Chapter Young Author Award (Dec. 2006), the Niwa Yasujirou Memorial Award (Feb. 2005), and the Young Researcher's Encouragement Award from the Japan chapter of the IEEE Vehicular Technology Society (VTS) (Oct. 2003). Dr. Taleb is an IEEE member.

M. Schöller received his MSc in Computer Science (Dipl.-Inform.) from Karlsruhe Universität in 2001. In 2006, he received his PhD from Karlsruhe Universität. Before joining the Next Generation Networking group at NEC Laboratories, he did a postdoctoral year at Lancaster University. His research interests
cover the fields of autonomous communication systems, resilient and survivable network architectures, wireless access technologies, and network security. Marcus has actively contributed to several national and European projects and published in key international conferences and journals.