

# Security in Wireless Mesh Networks

Editors

October 27, 2006



# Contents

<b>1</b>	<b>Attacks and Security Mechanisms</b>	<b>1</b>
1.1	Introduction . . . . .	1
1.2	Security Issues in Wireless Mesh Networks . . . . .	3
1.3	Attacks in Wireless Mesh Networks . . . . .	4
1.3.1	Physical Layer Attacks . . . . .	5
1.3.2	MAC Layer Attacks . . . . .	5
1.3.3	Network Layer Attacks . . . . .	8
1.3.4	Multi-radio Multi-channel Wireless Mesh Network Attacks . . . . .	12
1.4	Characteristics of Security Solution for Wireless Mesh Networks . . . . .	14
1.5	Security Mechanisms for wireless Mesh Networks . . . . .	15
1.5.1	MAC Layer Security Mechanisms . . . . .	16
1.5.2	Network Layer Security Mechanisms . . . . .	19
1.6	Towards Standardization . . . . .	21
1.6.1	Vulnerabilities in IEEE 802.11i and Security Attacks . . . . .	24

1.7	Open Issues . . . . .	28
1.8	Conclusion . . . . .	29

# Chapter 1

## Attacks and Security Mechanisms

Anjum Naveed, Salil S. Kanhere, Sanjay K. Jha  
School of Computer Science and Engineering  
University of New South Wales  
Sydney, Australia  
{anaveed,salilk,sjha}@cse.unsw.edu.au

The true potential of any network cannot be exploited without considering and adequately addressing the security issues. Wireless Mesh Networks (WMN), being multi-hop wireless networks, are prone to most of the security attacks on multi-hop wireless networks. In this chapter, we will discuss the security vulnerabilities in multi-hop wireless networks that are relevant to WMN. We will consider the attacks in WMN and the possible solution mechanisms to prevent and counteract these attacks.

### 1.1 Introduction

In recent years, WiFi (802.11) networks have become pervasive with numerous hotspots being deployed in urban city centers. However, in order to be connected, the mobile clients need to be within the radio range of the access point. To ensure that the target area is sufficiently

covered, ISPs would need to install additional hotspots in strategically placed locations to extend existing coverage. This may not always be possible due to constraints on the terrain, social issues, etc. Further, deploying additional hotspots adds to the installation cost and more importantly to the running costs (subscription cost for Internet connectivity for each access point). A promising, low-cost alternative for providing last-mile wireless connectivity is the concept of Wireless Mesh Networks (WMN). Wireless Mesh Networks (WMNs) are multi-hop wireless networks consisting of mesh routers and mesh clients. Generally, mesh routers have limited mobility and act as access points for the mobile clients to provide the connectivity over multiple hops as well as route the traffic for neighbouring mesh routers. Some of the routers are equipped with wired interface and serve the purpose of gateway to provide the connectivity with the Internet. The clients nodes may also act as intermediate hops for neighbouring nodes to extend the connectivity. A typical WMN architecture is shown in Figure 1.1. By enabling multi-hop communication between the mesh nodes, it is possible for several mobile clients to share a single broadband connection to the Internet. Several WMN deployments have been planned for major cities across the globe (Taipei, Moscow, Philadelphia, etc) in the near future. However, very little attention has been devoted by the research community to address the security issues in WMN.

The broadcast nature of transmission and the dependency on the intermediate nodes for routing the user traffic leads to security vulnerabilities making WMN prone to various attacks. The attacks can be external as well as internal in nature. External attacks are launched by intruders who are not part of the WMN and gain illegitimate access to the network. For example, an intruding node may eavesdrop the packets and replay those packets at a later stage of time to gain access to the network resources. Attacks from external nodes can be prevented by resorting to cryptographic techniques such as encryption and authentication. On the other hand, the internal attacks are launched by the nodes that are part of the WMN. One example of such attack is an intermediate node dropping the packets, which it was supposed to forward, leading to a denial of service attack. Similarly, the intermediate node may keep the copy of all the data that it forwards (internal eavesdropping) for offline processing and meaningful information retrieval without the knowledge of any other node in the network. Such attacks are typically launched either by selfish nodes or by malicious nodes, which may have been possibly compromised by attackers. There is a

subtle difference in their motives. The selfish node is seeking to greedily acquire greater than its fair share of the network resources at the expense of other users. On the contrary a malicious attacker's sole aim is to undermine the performance of the entire network. Note that in an internal attack, the misbehaving node is part of the WMN and hence has access to all the keying and authentication information. Consequently, cooperative mechanisms, which enable other nodes within the network to detect and possibly isolate these misbehaving nodes need to be employed.

It is evident that the true potential of WMN cannot be exploited without considering and adequately addressing the internal as well as the external security issues. In this chapter, we identify the security issues in WMN followed by the description of attacks on WMN. The primary focus will be the attacks that affect the MAC layer and the network layer of WMN. The characteristics of the security solution for WMN are identified and different solution mechanisms are discussed. The standardization efforts for the security in WMN are discussed. The chapter is concluded with some open issues yet to be considered in relation to security WMN.

## 1.2 Security Issues in Wireless Mesh Networks

Several vulnerabilities exist in the protocols for WMN that can be exploited by the attackers to degrade the performance of the network. The WMN nodes *depend on the intermediate nodes* for connectivity with other nodes in the network and the Internet. Consequently, the MAC layer protocols as well as the routing protocols for WMN assume that the participating nodes are well behaved with no malicious intentions. Therefore, all the nodes are assumed to follow the MAC protocol and perform the routing and packet forwarding operations as specified by the respective protocols. Based on this *assumed trust*, the nodes make independent decision for their transmission depending on the wireless channel availability. Similarly the routing protocols require the WMN nodes to exchange their routing information within the neighbourhood to make efficient routing decision. Since the nodes are assumed to be well behaved, each node makes an *independent decision* based on the routing protocol spec-

ifications. The node then informs its neighbours about the decision. The neighbour nodes neither verify the decision nor the information transmitted by the node. In practice however, some WMN nodes may behave in a *selfish* manner and/or other nodes may be compromised by *malicious* users. The *assumed trust* and the *lack of accountability* make the MAC layer protocols and the routing protocols vulnerable to various active attacks like black hole attack, wormhole attack and rushing attack [11, 12, 13].

The malicious or selfish nodes can drop data packets selectively or may chose to drop all the packets without forwarding any traffic. Further, since the participating nodes may not be owned by one administrator, specifically in case of community deployment of WMN, data confidentiality and data integrity can be compromised if the intermediate node keeps the copy of all the data for offline cryptanalysis and information retrieval. The malicious nodes may also *inject bad packets* in the network which may lead to DoS attack. Similarly, *passively sniffed packets* can be replayed at a later stage of time to gain access to the network resources. All these vulnerabilities render WMNs prone to security attacks. We consider the attacks on WMN that exploit these vulnerabilities in next section.

### 1.3 Attacks in Wireless Mesh Networks

In this section, the details of various attacks on WMN are given. We consider the attacks affecting the physical layer, MAC layer and the network layer because these layers form the core of the network. We do not consider the attacks on the transport and the application layers because these layers are primarily implemented in the end user devices hence the attacks on these layers are independent of the underlying network. Therefore the attacks and the counter-measures on these layers (Application and Transport) for WMN, other wireless networks or even wired networks would be same rather than being specific to WMN.

### 1.3.1 Physical Layer Attacks

All wireless networks including WMN suffer from radio jamming attack at the physical layer. The radio jamming attack [14] is a potentially damaging attack which can be launched with relative ease by simply allowing a wireless device to transmit a strong signal, which can cause sufficient interference to prevent packets in the victim network from being received. In its simplest form, the attacker may continuously transmit the jamming signal (constant jammer). Alternately, the attacker may resort to slightly sophisticated strategies whereby the attacker only transmits the radio signal when it senses some activity on the channel and remains quite otherwise (reactive jammer). However, these type of jamming attacks, where the transmission is an arbitrary signal, can be regarded as noise in the channel and MAC protocols like BMAC [15] can successfully counteract these attacks to a certain degree by adjusting the *signal-to-noise ratio (SNR)* threshold at the receiving node. More complex form of radio jamming attacks have been studied in [14] where the attacking devices do not obey the MAC layer protocol. We discuss these attacks in Section 1.3.2 as link layer jamming attacks.

### 1.3.2 MAC Layer Attacks

#### Passive Eavesdropping

The broadcast nature of transmission of the wireless networks make these networks prone to passive eavesdropping by the external attackers within the transmission range of the communicating nodes. Multi-hop wireless networks like WMN are also prone to internal eavesdropping by the intermediate hops whereby a malicious intermediate node may keep the copy of all the data, that it forwards, without knowledge of any other node in the network. Although passive eavesdropping does not affect the network functionality directly, it leads to the compromise in data confidentiality and data integrity. Data encryption is generally employed using strong encryption keys in order to protect the confidentiality and integrity of data.

### **Link Layer Jamming Attack**

Link layer jamming attacks are more complex as compared to blind physical layer radio jamming attacks. Rather than transmitting random bits constantly, the attacker may transmit regular MAC frame headers (no payload) on the transmission channel which conform to the MAC protocol being used in the victim network [16]. Consequently, the legitimate nodes always find the channel busy and back off for random period of time before sensing the channel again. This leads to the denial of service for the legitimate nodes and also enables the jamming node to conserve its energy resources. In addition to the MAC layer, jamming can also be used to exploit the network and transport layer protocols [17]. Intelligent jamming is not a purely transmit activity. Sophisticated sensors can be deployed, which detect and identify victim network activity, with a particular focus on the semantics of higher-layer protocols (e.g: AODV and TCP). Based on the observations of the sensor, the attacker can exploit the predictable timing behavior exhibited by higher-layer protocols and uses offline analysis of packet sequences to maximize the potential gain for the jammer. These attacks can be effective even if encryption techniques such as WEP and WPA have been employed. This is because the sensor that assists the jammer can still monitor the packet size, timing and sequence to guide the jammer. Since these attacks are based on carefully exploiting protocol patterns and consistencies across size, timing and sequence, preventing them will require modifications to the protocol semantics in such a way that these consistencies are removed wherever possible.

### **MAC Spoofing Attack**

MAC addresses have long been used as the singularly unique layer 2 network identifiers in both wired and wireless LANs. MAC addresses which are globally unique have often been used as an authentication factor or as a unique identifier for granting varying levels of network privileges to a user. This is particularly common in 802.11 WiFi networks. However, today's MAC protocols (802.11) and network interface cards do not provide for any safeguards that would prevent a potential attacker from modifying the source MAC address in its transmitted frames. On the contrary, there is often full support in the form of

drivers from manufacturers, which make this particularly easy. Modifying the MAC address in transmitted frames is referred to as MAC spoofing and can be used by attackers in a variety of ways. MAC spoofing enables the attacker to evade Intrusion Detection Systems (IDS) that are in place. Further, today's network administrators often use MAC addresses in access control lists. For example, only registered MAC addresses are allowed to connect to the access points. An attacker can easily eavesdrop on the network to determine the MAC addresses of legitimate devices. This enables the attacker to masquerade as a legitimate user and gain access to the network. An attacker can even inject a large number of bogus frames in to the network to deplete the resources (in particular bandwidth and energy) which may lead to denial of service for the legitimate nodes.

### **Replay Attack**

The replay attack, often known as the man-in-the-middle attack [18], can be launched by external as well as internal nodes. An external malicious node (not part of WMN) can eavesdrop the broadcast communication between two nodes (A and B) in the network as shown in Figure 1.2. It can then transmit these legitimate messages at a later stage of time to gain access to the network resources. Generally, the authentication information is replayed where the attacker deceives a node (node B in Figure 1.2) to believe that the attacker is a legitimate node (node A in Figure 1.2). On a similar note, an internal malicious node, which is an intermediate hop between two communicating nodes, can keep a copy of all relayed data. It can then retransmit this data at a later point in time to gain the unauthorized access to the network resources. The replay attack, exploiting the IEEE 802.1X [33] authentication mechanism is discussed in Section 1.6.

### **Pre-computation and Partial Matching Attacks**

In this section we discuss a different form of security attacks. Unlike above mentioned attacks where MAC protocol vulnerabilities are exploited, these attacks exploit the vulnerabilities in the security mechanisms that are employed to secure the MAC layer of the network.

Pre-computation and partial matching attacks exploit the cryptographic primitives that are used at MAC layer to secure the communication. In a pre-computation attack or (Time Memory Trade Off attack (TMTO)), the attacker computes a large amount of information (key, plain text and respective cipher text) and stores that information before launching the attack. When the actual transmission starts, the attacker uses the pre-computed information to speed up the cryptanalysis process. TMTO attacks are highly effective against a large number of cryptographic solutions. On the other hand, in a partial matching attack, the attacker has access to some (cipher text, plain text) pairs, which in turn decreases the encryption key strength and improves the chances of success of the brute force mechanisms. Partial matching attack exploits the weak implementations of encryption algorithms. For example, in IEEE 802.11i standard for MAC layer security in wireless networks [30], the MAC address fields in MAC header are used in the message integrity code (MIC). The MAC header is transmitted as plain text while the MIC field is transmitted in the encrypted form. Partial knowledge of the plain text (MAC address) and the cipher text (MIC) makes IEEE 802.11i vulnerable to partial matching attack.

Denial-of-Service (DoS) attacks may also be launched by exploiting the security mechanisms. For example, IEEE 802.11i standard for MAC layer security in wireless networks is prone to the *session hijacking attack* and the *man-in-the-middle attack* exploiting vulnerabilities in IEEE 802.1X and *DoS attack* exploiting vulnerabilities in four-way handshake procedure in IEEE 802.11i. Although these attacks are also considered as MAC layer attacks, we postpone the discussion on IEEE 802.11i, its vulnerabilities, attacks exploiting these vulnerabilities and the proposed prevention mechanisms till Section 1.6.

### 1.3.3 Network Layer Attacks

The attacks on the network layer can be divided into control plane attacks and data plane attacks and can be active or passive in nature. Control plane attacks generally target the routing functionality of the network layer. The objective of the attacker is to make routes unavailable or force the network to choose sub-optimum routes. On the other hand, the data plane attacks affect the packet forwarding functionality of the network. The objective

of the attacker is to cause the denial of service for the legitimate user by making user data undeliverable or injecting malicious data into the network. We first consider the network layer control plane attacks followed by the discussion on network layer data plane attacks.

### Control Plane Attacks

*Rushing attacks* [11] targeting the on-demand routing protocols (e.g: AODV) were among the first exposed attacks on the network layer of multi-hop wireless networks. Rushing attack exploits the route discovery mechanism of on-demand routing protocols. In these protocols, the node requiring the route to the destination floods the **Route Request** message which is identified by a sequence number. To limit the flooding, each node only forwards the first message that it receives and drops remaining messages with same sequence number. The protocols specify a specific amount of delay between receiving the **Route Request** message by a particular node and forwarding it, to avoid collusion of these messages. The malicious node launching the rushing attack forwards the **Route Request** message to the target node before any other intermediate node from source to destination. This can easily be achieved by ignoring the specified delay. Consequently, the route from source to destination includes the malicious node as intermediate hop which can then drop the packets of the flow resulting in data plane denial of service attack.

*Wormhole attack* has a similar objective albeit uses a different technique [12]. During a wormhole attack, two or more malicious nodes collude together by establishing a tunnel using an efficient communication medium (i.e. wired connection or high speed wireless connection etc) as shown in Figure 1.3. During the route discovery phase of on-demand routing protocols, The **Route Request** messages are forwarded between the malicious nodes using the established tunnel. Therefore, the first **Route Request** message that reaches the destination node is the one forwarded by the malicious nodes. Consequently, the malicious nodes are added in the path from source to destination. Once the malicious nodes are included in the routing path, the malicious nodes either drop all the packets resulting in complete denial of service or drop the packets selectively to avoid detection.

*Black hole attack* (or sink hole attack) [19] is another attack that leads to denial of service in wireless mesh networks. It also exploits the route discovery mechanism of on-demand routing protocols. In a black hole attack, the malicious node always replies positively to a **Route Request** although it may not have a valid route to the destination. Since the malicious node does not check its routing entries, it will always be the first to reply the **Route Request** message. Therefore, almost all the traffic within the neighbourhood of the malicious node will be directed towards the malicious node which may drop all the packets resulting in denial of service. Figure 1.4 shows the effect of a black hole attack in the neighbourhood of the malicious node where all the traffic is directed towards the malicious node. A more complex form of the attack is the cooperative black hole attack where multiple malicious nodes collude together resulting in complete disruption of routing and packet forwarding functionality of the network. The cooperative black hole attack and their prevention mechanisms have been studied in [13].

*Grey hole attack* is a variant of the black hole attack. In a black hole attack, the malicious node drops all the traffic that it is supposed to forward. This may lead to possible detection of the malicious node. In a grey hole attack the adversary avoids the detection by dropping the packets selectively. Grey hole attack does not lead to complete denial of service but it may go undetected for a longer duration of time. This is because the malicious packet dropping may be considered as the congestion in the network which also leads to selective packet loss.

*Sybil Attack* is the form of attack where malicious node creates multiple identities in the network, each appearing as a legitimate node [20]. Sybil attack was first exposed in distributed computing applications where the redundancy in the system was exploited by creating multiple identities and controlling the considerable system resources. In the networking scenario, a number of services like packet forwarding, routing and collaborative security mechanisms can be disrupted by the adversary using sybil attack. Following form of the attack effects the network layer of WMN. WMN are supposed to take advantage of the path diversity in the network to increase the available bandwidth and reliability. If the malicious node creates multiple identities in the network, the legitimate nodes, assuming these identities to be distinct network nodes, will add these identities in the list of distinct paths

available to a particular destination. When the packets are forwarded to these fake nodes, the malicious node, that created the identities, processes these packets. Consequently, all the distinct routing paths will pass through the malicious node. The malicious node may launch any of the above mentioned attacks. Even if no other attack is launched, the advantage of path diversity is diminished, resulting in degraded performance.

In addition to the above mentioned attacks, the wireless mesh networks are also prone to *network partitioning attack* and *routing loop attack*. In network partitioning attack, the malicious nodes collude together to disrupt the routing tables in such a way that the network is divided into non-connected partitions resulting in denial of service for certain network portion. Routing loop attacks affect the packet forwarding capability of the network where the packets keep circulating in loop until they reach the maximum hop count, at which stage the packets are simply discarded.

### Data Plane Attacks

Data plane attacks are primarily launched by the selfish and malicious (compromised) nodes in the network and lead to performance degradation or the denial of service for the legitimate user data traffic. The simplest of the data plane attacks is *passive eavesdropping*. Eavesdropping has already been discussed in Section 1.3.2 as a MAC layer attack and we do not discuss it further. Selfish behavior of the participating WMN nodes is a major security issue because the WMN nodes are dependent on each other for data forwarding. The intermediate hop selfish nodes may not perform the packet forwarding functionality as per the protocol. The selfish node may drop all the data packets resulting in complete denial of service or it may drop the data packets selectively or randomly. It is hard to distinguish between such a selfish behavior and the link failure or network congestion. On the other hand, malicious intermediate hop nodes may inject junk packets into the network. Considerable network resources (bandwidth and packet processing time) may be consumed to forward the junk packets which may lead to denial of service for the legitimate user traffic. The malicious nodes may also inject the maliciously crafted control packets which may lead to the disruption of routing functionality. The control plane attacks are dependent on such maliciously

crafted control packets. The malicious and selfish behavior has been studied in [22, 23].

#### 1.3.4 Multi-radio Multi-channel Wireless Mesh Network Attacks

In this section, we consider the attacks that affect the network layer as well as the MAC layer of WMN. These attacks exploit the channel assignment and routing algorithms in multi-radio multi-channel wireless mesh networks (MR-MC WMN). Bandwidth capacity is a major limitation for wireless mesh networks. In MR-MC WMN, each WMN node is equipped with multiple radios (NICs) to increase the available bandwidth. Orthogonal channels are used for each interface of the node which ensures simultaneous communication using all the wireless interfaces without interference. Dynamic channel assignment is required to assign the channels to the network links. The objective of the channel assignment algorithms is to ensure the minimum interference within WMN. Various joint routing and channel assignment algorithms have been proposed for (MR-MC WMN) [1, 2, 3, 4, 5]. Readers are encouraged to review the dynamic routing and channel assignment algorithms proposed in [2] for better understanding of the attacks discussed in this section. Note that channel assignment is done at the MAC layer while the routing is a network layer functionality. All the joint routing and channel assignment algorithms assume that the mesh nodes are well-behaved. Hence the nodes make independent decision about their channel assignment based on the neighbour channel assignment information and inform neighbouring nodes about the decision which is not verified. The assumed trust amongst the WMN nodes and the independent decision of the nodes make these algorithms vulnerable to security attacks.

*Network endo-parasite attack (NEPA)* [21] is launched by the compromised malicious node when it changes the channel assignment of its interfaces in such a way that the interference on heavily loaded high priority channels increases (Each interface is switched to a different high priority channel). This is contrary to the normal operation of the channel assignment algorithm where the node assigns the least loaded channels to its interfaces. Figure 1.5 shows the attack. The malicious node 'F' has switched the channel on link 'FH' to the same channel as the link 'GC' and link 'FI' to the channel used by link 'GD'. The malicious switching by node 'F' will increase the interference on links 'GC' and 'GD'. The malicious

node does not inform its neighbours about the change in channel assignment, therefore, the neighbouring nodes are unable to adjust their channel assignment in order to mitigate the effect of increased interference. The increase in interference results in serious performance degradation.

*Channel ecto-parasite attack (CEPA)* [21] is a special type of NEPA. During CEPA, the malicious node switches all its interfaces to the most heavily loaded highest priority channel. Like NEPA, the malicious node does not inform its interference domain neighbours about the change in channel assignment. The effect of the attack is the hidden usage of the most heavily loaded channel which increases the interference considerably resulting in a decrease in performance. The attack is shown in Figure 1.6 where the malicious node has switched both its child links 'FH' and 'FI' to the channel that is being used by the high priority link 'GC'. As the links 'FH' and 'FI' are within the interference range of the link 'GC', the link 'GC' will experience high interference. However the malicious node has not informed its neighbours about the change in channel assignment, therefore, the node 'G' will continue to use same channel on link 'GC' assuming the external noise or other factors to be the reason for degraded performance.

*Low cost ripple effect attack* [21] is launched when the compromised malicious node transmits misleading channel assignment information about its interfaces to the neighboring nodes without actually changing the channel assignment. The information is calculated in such a way that the neighboring nodes are forced to adjust their channel assignments in order to minimize the interference which may generate a series of changes even in the channel assignment of the nodes that are not direct neighbors of the malicious node. The effect of the attack is shown in Figure 1.7 using the bold arrow. Although most of the dynamic channel assignment algorithms prevent the ripple effect to propagate within the network from the parent nodes (closer to the wired gateway) to the child nodes, the effect can still propagate in the reverse direction. The objective of the attack is to force the network in the quasi-stable state by imposing premature channel adjustment on other nodes repeatedly. Considerable network resources are consumed for channel adjustment and the user data forwarding capability is severely affected. The attack is relatively more severe than NEPA and CEPA because the effect is propagated to a large portion of the network even beyond the

neighbours of the compromised node, disrupting the traffic forwarding capability of various nodes for considerable time duration.

## 1.4 Characteristics of Security Solution for Wireless Mesh Networks

In the previous section, we discussed the security attacks that exploit the vulnerabilities in the MAC layer and the network layer protocols for WMN. We now enlist the essential characteristics that a security mechanism for WMN should have, in order to successfully prevent, detect and counteract these attacks. We only enlist the characteristics that differentiate WMN security mechanisms from existing security mechanisms for wired and wireless networks.

- In wired networks, the security services of data confidentiality and data integrity are generally provided on a per link basis (between two devices). This is based on the assumption that the end devices are secure. However, as discussed in previous sections, the WMN nodes may resort to the selfish and malicious behavior. To counteract the selfish and malicious behavior of the intermediate hop nodes, the WMN must provide the end-to-end services of data confidentiality and data integrity, in addition to the security services on per link basis.
- The trust establishment mechanism should be robust against internal selfish and malicious behaviour. Note that the internal selfish and malicious nodes are part of WMN therefore the conventional authentication mechanisms based on cryptographic primitives may not be effective against the internal misbehaviour.
- Section 1.3.3 and Section 1.3.4 indicate that the accountability should be a necessary characteristic for WMN to ensure that the WMN nodes behave according to the protocol specification even if the nodes take independent decision about routing and channel assignment.
- Wireless mesh networks are self administered networks and lack the centralized admin-

istration authority which can respond to the network issues. Therefore, the attack and anomaly detection mechanisms for wireless mesh networks should be self sufficient and must not be dependent on the administrator to verify the possible attack and anomaly alerts.

- An important characteristic of wireless mesh networks is the self healing nature. Therefore, the detection mechanisms must be coupled with adequate automated response to the security attacks and identified anomalies.

Having identified the essential characteristics of the security mechanisms for wireless mesh networks, we now consider different security mechanisms that are employed to counteract the attacks identified in Section 1.3.

## 1.5 Security Mechanisms for wireless Mesh Networks

ITU-T Recommendation X.800 [29] - Security Architecture for OSI - defines the required security services for communication networks. The security services have been broadly categorized into five groups namely authentication, access control or authorization, confidentiality, integrity and non-repudiation. Security management services have also been defined aimed at ensuring the availability, accountability and event management. The security services can be categorized into two broad categories of intrusion prevention and intrusion detection. In case of intrusion prevention, measures are taken to stop the attacker from intruding into the network and launching the attack on the network. The protection can be from external as well as the internal intruders. Security services of authentication, access control, data confidentiality, data integrity and non-repudiation lead to intrusion prevention. However, intrusion prevention is insufficient to protect the network from all attacks because no prevention technique can ensure the complete protection. Therefore, the intrusion prevention mechanisms are complimented by intrusion detection and response mechanisms. The role of intrusion detection is to identify the illegitimate activities which may be the consequence of the attacks or may lead to the attacks. Early detection and timely response can limit the effect of the attack on the network. The intrusion detection and response mechanisms aim

at ensuring the accountability and availability of the network services. Figure 1.8 shows how different security services fit together in the security model for wireless mesh networks. We now consider the intrusion prevention mechanisms as well as intrusion detection mechanisms both at the MAC layer and the network layer of wireless mesh networks.

### 1.5.1 MAC Layer Security Mechanisms

#### Intrusion Prevention Mechanisms

Various security frameworks [30, 31, 32] have been proposed for multi-hop wireless networks that are applicable to wireless mesh networks with slight modification. These security frameworks provide the security services of authentication, data confidentiality and data integrity at MAC layer of the network on per link basis. Most of the security frameworks employ the *cryptographic primitives*. For example, Soliman and Omari [31] have proposed the security framework based on stream cipher for encryption to provide the services of data confidentiality, data integrity and authentication. The objective of using stream cipher is to allow the online processing of the data. Consequently, minimum delay is introduced because of the security provisioning. Two secret security keys, Secret Authentication Key (SAK) and Secret Session Key (SSK) are used for authentication of the supplicant and authenticator. SAK is exchanged between the supplicant and the authenticator after initial mutual authentication from the authentication server whereas the SSK is used for a given communication session between the two nodes. The SAK and SSK pair is used by the communicating nodes to generate the permutation vector (PV) which is used for the encryption and decryption of data. In the strongest mode of security, the data is also involved in the PV generation. The synchronization of the generated permutation vector between the sender and the receiver of the data results in origin authentication of every MPDU. To minimize the security overhead, plain text MPDU is XORed with the PV generated for that MPDU. The authors have proved that the encryption of data using PV provides strong security services of data confidentiality, data integrity and origin authentication.

IEEE 802.11i was ratified in June 2004 as the standard for the security of the MAC

layer of the wireless networks. The standard is based on the cryptographic primitives and provides the services of data confidentiality, data integrity and authentication. The standard is discussed in detail in Section 1.6.

One of the major security requirements in case of multi-hop wireless networks like WMN is the trust establishment between communicating nodes. As mentioned in Section 1.4, conventional cryptography based mechanisms are generally non-applicable to multi-hop networks like WMN. Consequently, a number of distributed neighbour collaboration authentication protocols have been proposed by researchers for this purpose [38, 39, 42]. A comprehensive analysis of the authentication protocols for wireless networks can be found in [41]. Deng et. al. [42] have proposed the threshold and identity-based authentication and key management for multi-hop wireless networks. Threshold cryptography based solution is proposed for the distribution of the master key  $\langle$ public key, private key $\rangle$  and the authentication of the nodes based on the private key. In the proposed scheme, all nodes possess the public key while every node has got a share of the private key.  $(k,n)$  threshold secret sharing is employed to generate the private key for the node which states that 'k' out of 'n' shares of private key are required to construct the complete private key and less than 'k' shares of the secret key cannot construct the complete private key. Based on this mechanism, whenever a node needs to refresh its private key, it needs 'k' neighbours to send their secret share to the node to reconstruct the private key and no node can construct the private key based on its own information. The process of private key generation is shown in the Figure 1.9 where the requesting node broadcasts the request message along with its own share for verification. The neighbouring nodes reply the request message by sending their own share of secret key to the requesting node. The requesting node is able to generate the private key on receiving 'k' shares of the key. In this way, the intruding node cannot generate the private key unless its own share of private key is verified by 'k' neighbouring nodes. Similarly, the private key of the misbehaving node is not refreshed by the neighbours. Therefore, the threshold secret sharing serves as the strong authentication and key management solution.

The security mechanisms discussed above prevent the network from MAC layer attacks as follows. The security service of data confidentiality leads to the protection against passive eavesdropping attack. Although the nodes within the transmission range of the communi-

cating nodes can still overhear the communication, the data is protected using encryption mechanisms provided by the data confidentiality service. Therefore the received information is useless, unless it is decrypted using brute force methods which are impractical keeping the value of information retrieved versus the cost of attack. Data and header integrity service provides the protection against MAC spoofing attacks. The message with spoofed MAC address (IP address for IP spoofing) will fail the integrity check at the receiving node and will be discarded. Per packet authentication and integrity provided by the solutions like [30, 31] protect the data against replay attacks. These solutions use a fresh key for each message which is synchronously computed by sender and the receiver. Therefore, a replayed packet, encrypted using outdated key will fail the integrity check and will be discarded. Use of fresh key for each message also protects the data from pre-computation and partial matching attacks because the pre-computed information needs to be applied on every message in order to decrypt that message. This renders the attack extremely costly as compared to the information retrieved.

### **Intrusion Detection Mechanisms**

Very few intrusion detection systems have been proposed at the MAC layer of wireless networks. Lim et. al. [43] have proposed an intrusion detection system to secure wireless access points coupled with automated active response. Authors have proposed the deployment of specific detection devices closer to wireless access points and the detection is done at the MAC layer. RTS/CTS (Ready To Send/Clear To Send) messages from the blacklisted MAC addresses are proposed as detection metrics. As a response to the intrusion, authors propose the use of the intruder's tactics back onto the intruder by crafting and transmitting the malformed packets back. The proposed idea of deploying dedicated detection devices may not be cost affective. Similarly, the response mechanism may be computation resource extensive. Further, the legitimate nodes may get punished if the detected information is not accurate.

One of the most recent works in this context is from Liu et. al. [24]. The authors have proposed the game theoretic approach for selecting the optimum intrusion detection strategy

at a given instance from a set of deployed weak intrusion detection mechanisms. The basic idea is that different intrusion detection techniques are very good at detecting certain type of attacks while do not perform optimally in other cases. The combination of these strategies and the use of optimum strategy in a given scenario can increase the detection accuracy of the resulting system. However, while the idea of selecting the optimum technique at a given instance has strength, basically at a given instance of time, only one weak intrusion detection technique will be used. Consequently, the performance of intrusion detection may not significantly improve as compared to the increase in overhead because of the IDS selection mechanism.

The intrusion detection mechanisms at the MAC layer are used to detect the attacks launched by misbehaving nodes that do not obey the MAC layer protocol. These attacks include the link layer jamming attacks and denial of service attacks.

### 1.5.2 Network Layer Security Mechanisms

#### Intrusion Prevention Mechanisms

Intrusion prevention techniques have been proposed to secure the routing protocols for multi-hop wireless networks. These protocols include Secure Routing Protocol (SRP) [6], Secure AODV (SAODV) [7], Authenticated Routing for Ad hoc Network (ARAN) [8] and Ariadne; A secure On-demand routing protocol [9] to list a few. The most recent work in this domain is [10]. All these protocols use cryptographic primitives to establish some form of trust between the network nodes through the process of mutual authentication. For example, Secure Routing Protocol (SRP) [6] is aimed as securing the route discovery process and safeguards the routing functionality from attacks exploiting the routing protocol itself. The `Route Request` and `Route Reply` messages are protected by message authentication code (MAC) for authentication of the originating node. The IP address of the intermediate nodes is also added in the `Route Request` message for cross validation in order to prevent the network from attacks like black hole and wormhole. Authors prove that the protection of `Route Request` and `Route Reply` message ensures protection against multiple attacks

except for the case where multiple nodes collude together and launch the attack. SAODV [7] uses digital signatures to authenticate all the fields of `Route Request` and `Route Reply` messages except from the hop count field. Digital signatures are used on end-to-end basis between source and destination. the hop count field is secured using hash chains on per link basis.

The intrusion prevention mechanisms are primarily used to establish the trust between the participating nodes and providing the control message integrity and confidentiality. These services can provide some protection against wormhole attack and black hole attack. However, the problem of malicious and misbehaving nodes cannot be addressed completely using the intrusion prevention mechanisms at the network layer and the support from intrusion detection mechanisms becomes mandatory.

### **Intrusion Detection Mechanisms**

Numerous intrusion detection techniques have been proposed at the network layer for wired as well as wireless networks. In this section we briefly discuss some of the recent research efforts in this domain, however, the survey by no means is exhaustive. Most of the intrusion detection systems rely on the knowledge based systems and data mining techniques [25, 26, 27, 28]. For example Huang et. al. [26] have proposed IDS for multi-hop mobile wireless networks based on the cross-feature analysis. The nodes monitor different parameters in the network and based on values of  $i - 1$  parameters, predict the value of  $ith$  parameter and compare it with monitored value of that parameter to detect routing anomalies in the networks. Authors have also proposed the distributed cluster based approach as an extension to this work [27] where they propose the division of network into clusters and only few elected nodes within each cluster perform the monitoring with the intrusion detection probability almost same as with all the nodes actively monitoring. This scheme is resource efficient which is the primary design goal for wireless networks.

Yang et. al. [28] has proposed the self organized network layer security solution for mobile ad hoc networks. This is one of the very few solutions which ensure self healing and self organized network. The solution is based on distributed neighbour collaboration and

information cross-validation, resulting in self organized/self healing network. The scheme is based on the threshold secret sharing discussed in Section 1.5.1 which is used to refresh the token of the nodes. Authors have proposed a novel token based crediting scheme. The token of the node expires after some time duration. The token expiry time of the node depends upon the credit of the node. The credit of the well behaving nodes gets accumulated over the period of time. Therefore, the token expiry time of these nodes is longer and is linearly incremented every time the node refreshes its token. The token of malicious or selfish nodes is revoked by neighbour collaboration refraining them to participate in the network. The detection metrics used to differentiate between well behaving and malicious nodes are based on the routing protocols and consist of hop count distance, packet forwarding ratio etc.

The intrusion detection mechanisms at the network layer primarily address the issues of malicious, selfish and misbehaving nodes that are at the heart of almost all the attacks at network layer. The solutions like [26, 27, 28] identify the anomalies in the control messages to detect the control plane attacks like rushing attack, wormhole attack, black hole attack, grey hole attack, network partitioning attack and routing loop attack. On the other hand, neighbour monitoring techniques [26, 27] are employed to detect the data plane attacks.

## 1.6 Towards Standardization

IEEE 802.11i [30] is the defined standard for the MAC layer security of the wireless networks. The draft standard for wireless mesh networks, IEEE 802.11s, has proposed the use of IEEE 802.11i for the MAC layer security in wireless mesh networks. Therefore, we dedicate this section to discuss the IEEE 802.11i standard. We first explain the security methods used and the security services provided in the IEEE 802.11i standard. In the later part of the section we will expose the vulnerabilities in IEEE 802.11i that render the standard prone to security attacks. These attacks include the pre-computation and partial matching attacks, session hijacking attack and the man-in-the-middle attack exploiting vulnerabilities in IEEE 802.1X and DoS attack exploiting vulnerabilities in four-way handshake. We also discuss the proposed prevention mechanisms for these attacks briefly.

IEEE 802.11i provides the security services of data confidentiality, data integrity, authentication and protection against replay attacks. The standard consists of three components: Key Distribution component, Mutual Authentication component, Data Confidentiality Integrity and Origin Authentication component. In the following paragraphs, we briefly discuss these components.

IEEE 802.1X [33] is used for *key distribution and authentication*, entailing the use of Extensible Authentication Protocol (EAP) [34] and an authentication, authorization, and accounting server (AAA Server) like RADIUS or DIAMETER [35, 36]. IEEE 802.1X is a port-based access control protocol which operates in client-server architecture. When the router/access point (authenticator) detects a new client (supplicant), the port on the authenticator is enabled and set to the "unauthorized" state for that client. In this state, only 802.1X traffic (EAP messages) is allowed and all other traffic is blocked from that client. The authenticator sends out the EAP-Request message to the supplicant, the supplicant replies with the EAP-Response message. The authenticator forwards this message to the AAA server. If the server authenticates the client and accepts the request, it generates Pairwise Master Key (PMK) which is distributed to authenticator and supplicant using EAP messages. After authentication from server, the authenticator sets the port for the client to the "authorized" state and normal traffic is allowed. Note that the same protocol can be used to authenticate and distribute keys between two peer routers or two peer clients in case of wireless mesh networks.

Encryption key distribution (PMK) and authentication using 802.1X is followed by *mutual authentication* of supplicant (client or peer router) and authenticator (Router/AP or peer router) which is based on the four-way handshake. The four-way handshake is initiated when the two nodes intend to exchange data. The encryption key distribution makes the shared secret key PMK available to the supplicant as well as the authenticator. This key is however designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish two more keys called the Pairwise Transient Key (PTK) and Group Temporal Key (GTK). PTK is generated by the supplicant by concatenating the PMK, Authenticator nonce (ANonce), Supplicant nonce (SNonce), Authenticator MAC address and Supplicant MAC address. The product is then put through a

cryptographic hash function. GTK is generated by authenticator and transmitted to supplicant during four-way handshake. PTK is used to generate Temporal Key (TK) which is used to encrypt unicast messages while the GTK is used to encrypt broadcast and multicast messages. The four-way handshake (shown in Figure 1.10) involves generation and distribution of these keys between supplicant and authenticator resulting in the mutual authentication. The first message of the four-way handshake is transmitted by the authenticator to the supplicant which consists of ANonce. The supplicant uses this ANonce and readily available fields with itself to generate the PTK. The second message of the handshake is transmitted by the supplicant to the authenticator consisting of SNonce and Message Integrity Code (MIC) which is encrypted using PTK. The authenticator is then able to generate the PTK and GTK. The attached MIC is decrypted using the generated PTK. If the MIC is successfully decrypted, then the authenticator and the supplicant have successfully authenticated each other (Mutual Authentication). This is because the authenticator's generated PTK will only match the PTK transmitted by the supplicant if the two share the same PMK. Third message is transmitted by the authenticator consisting of GTK and MIC. The Last message of four-way handshake is the acknowledgement transmitted by the supplicant. The two nodes can exchange the data after successful four-way handshake.

IEEE 802.11i provides two methods for the security services of *data confidentiality, data integrity, origin authentication and protection against replay attacks*. First method, Temporal Key Integrity Protocol (TKIP) is the enhanced version of Wired Equivalent Privacy (WEP) and has been provided for backward compatibility with the hardware that was designed to use WEP. RC4 encryption has been used as encryption algorithm, however, the implementation of algorithm is weak rendering the protocol vulnerable to numerous security attacks. We do not discuss this method in detail. Interested readers are referred to the Section 8.3.2 of the standard [30] for further details of the method.

The second method is the Counter mode (CTR) with CBC-MAC Protocol (CCMP). CCMP is based on the Counter mode With CBC-MAC (CCM) [37] of the AES encryption algorithm. CCM combines Counter (CTR) for confidentiality and the Cipher Block Chaining (CBC) Message Authentication Code (MAC) for origin authentication and integrity. As shown in Figure 1.11 CCM encryption takes four inputs: The Encryption key, Additional

Authentication Data (AAD), a unique Nonce for every frame and the Plain text. CCM requires a fresh temporal key (TK) (Generated from PTK) for every session which is used as encryption key. AAD is constructed from the MAC header. It consists of the following fields from MAC header: Frame Control field FC (Certain bits masked), Address A1, Address A2, Address A3, Sequence Control field SC (Certain bits masked), Address A4 (If present in the MAC header) and Quality of service Control field QC (if present). CCMP uses the A2 and the priority fields of MAC header along with a 48-bit Packet Number (PN) to generate the unique nonce value for each frame protected by a given TK. PN is incremented for each MAC Protocol Data Unit (MPDU) resulting in a fresh value of nonce for each MPDU. The output of the encryption is the cipher text and the Message Integrity Code (MIC). The frame to be transmitted is constructed by concatenating the MPDU header, CCMP header, cipher text and MIC. CCM encryption is explained in RFC 3610.

### 1.6.1 Vulnerabilities in IEEE 802.11i and Security Attacks

IEEE 802.11i standard successfully provides a number of security services, however, a number of security vulnerabilities have been identified in the recent years. We discuss these vulnerabilities, the attacks exploiting these vulnerabilities and the available prevention mechanisms in this sub section.

#### IEEE 802.1X Vulnerabilities

IEEE 802.1X [33] is used by IEEE 802.11i standard for key distribution and authentication. Three entities namely; Authenticator, Supplicant and the Authentication server participate in the process. The basic assumption underlying the protocol is that the authenticator is always trusted. Therefore, the supplicant do not verify the messages received from the authenticator and unconditionally responds to these messages. However in practice, the adversary can also act as authenticator which renders the protocol vulnerable to the session hijacking attack and the man-in-the-middle attack as exposed in [45]. Figure 1.12 shows, how an adversary can exploit the above mentioned vulnerability to launch session hijacking

attack. The adversary waits until the authenticator and the supplicant complete the authentication process and the authenticator send the EAP success message to the supplicant. Following this, the adversary sends 802.11 disassociate message to the supplicant with the spoofed IP of the authenticator. The supplicant assumes its session has been terminated by the authenticator as the message is not verified for integrity. The adversary gains the access to the network by spoofing the MAC address of supplicant and proceeds with mutual authentication procedure using four-way handshake.

Figure 1.13 shows man-in-the-middle attack launched by the adversary exploiting the vulnerability in IEEE 802.1X. After the initial exchange of EAP request and response messages between the supplicant and the authenticator, the adversary sends EAP success message to the supplicant using its own MAC address. Since the IEEE 802.1X protocol suggests unconditional transition upon receiving the EAP success message by the supplicant, the supplicant assumes it is authenticated by the authenticator and changes the state. When the authenticator sends the EAP success message, the supplicant has already passed the stage where it was waiting for the success message and hence no action is taken for this message. The supplicant assumes the adversary as the legitimate authenticator while the adversary can easily spoof the MAC address of the supplicant to communicate with the actual authenticator. Therefore, the adversary will become the intermediary between the supplicant and the authenticator. The proposed solutions to prevent these attacks [45] recommend the authentication and integrity check for the EAP messages between the authenticator and the supplicant. The solution also proposes that the peer-to-peer based authentication model be adopted where the authenticator and the supplicant should be treated as peers and the supplicant should verify the messages from the authenticator during the process of trust establishment. The peer-to-peer model is suitable for WMN where both the authenticator and the supplicant are WMN routers.

### **Four-way Handshake Vulnerabilities**

Four-way handshake is the mechanism used for the mutual authentication of the supplicant and the authenticator in IEEE 802.11i. Vulnerabilities in the four-way handshake have been

identified and the DoS attack exploiting these vulnerabilities proposed in [44]. The handshake starts after PMK is distributed to the supplicant and the authenticator. The supplicant waits for a specific interval of time for message 1 of the handshake from the authenticator. If the message is not received, the supplicant disassociates itself from the authenticator. Note that this is the only timer used by the supplicant. If message 1 is received by the supplicant, it is then bound to respond to every message from the authenticator and wait for the response until it is received. On the other hand, the authenticator will timeout for every message, if it does not receive the expected response within a specific time interval. Further, the supplicant is de-authenticated if the response is not received after several retries. Also note that both the authenticator and the supplicant drop the message silently, if the MIC of the message cannot be verified.

This mechanism of four-way handshake is vulnerable to the DoS attack by the adversary. Consider Figure 1.14 where the authenticator sends the message 1 to the supplicant. Note that message 1 is not encrypted. Supplicant generates a new SNonce and then generates PTK using the ANonce, SNonce and other relevant fields and responds with the message 2 which is encrypted using PTK. At this point, the adversary sends the malicious message 1 with the spoofed MAC address of the authenticator. The supplicant is bound to respond to the message. It assumes that the message 2 that it sent to the authenticator is lost so the authenticator has retransmitted the message 1. Therefore, it calculates PTK' (different from PTK and over writing PTK) based on the ANonce sent by adversary and sends message 2 again which is encrypted using PTK'. Meanwhile, the authenticator responds to the first message 2 of the supplicant by sending the message 3 which is encrypted using PTK. The integrity check performed by the supplicant on message 3 fails because the supplicant is now using PTK' while the authenticator encrypted the message using PTK. Consequently the four-way handshake process is blocked until the authenticator de-authenticates the supplicant after several retries, denying the supplicant of the service.

Three solutions have been proposed in [44] to prevent the above attack. We only discuss the most effective solution here. Note that every time the supplicant receives message 1, it generates a new SNonce which is concatenated with ANonce (transmitted by authenticator in message 1) and other relevant information to generate new PTK. The proposed solution

suggests that the supplicant should store the SNonce created in response to the first message 1 that it receives from authenticator. Same SNonce should be used for all subsequent message 1s until the supplicant receives message 3 from the authenticator. Upon receiving the message 3, supplicant should use the newly transmitted ANonce in message 3 and the stored SNonce to generate PTK again, which should be used to decrypt message 3. Use of same SNonce and ANonce will generate same PTK if other information remains unchanged. Therefore, supplicant will be able to respond to the legitimate message 3 even if it receives multiple message 1s from adversary. Note that the adversary cannot send a malicious message 3 because message 3 is encrypted using PTK which is dependent on PMK (only known to the supplicant and the authenticator).

### **CCMP Encryption Vulnerabilities**

Although CCMP (employed by IEEE 802.11i) uses the CCM encryption, the strength of which is time tested, the protocol is vulnerable to the partial matching and pre-computation attacks. The vulnerabilities of the protocol implementation and the resulting attacks have been exposed in [40]. The research shows that the address field A2 and the priority field of the MAC header and the PN field in the CCMP header are transmitted as plain text in the headers as well as in the encrypted form as part of the MIC. This leads to the partial matching attack and the researchers have shown that the key strength of the 128-bit encryption key used in CCMP decreases. The decrease in the key strength exposes the protocol to pre-computation attack resulting in the compromise of data confidentiality and data integrity. Further, The CCM encryption is a two phase process. During first phase the MIC is calculated and in second phase the encryption of the frame takes place. Similarly, the decryption is done in two phases where first the message integrity is verified from MIC and then the decryption takes place. The two phase processing of the frame at each wireless link may lead to considerable delay in case of multi-hop wireless networks like wireless mesh networks where the data traverses a number of intermediate wireless hops before reaching the wired Internet. The delay introduced by the security services leads to the impracticability of the CCMP protocol for large wireless mesh networks consisting of several intermediate hops.

## 1.7 Open Issues

A number of security solutions have been discussed aimed at solving different security issues, preventing, detecting and counteracting the security attacks however, a number of open issues still require considerable attention.

- Quite a few intrusion detection systems exist for multi-hop wireless networks however, very few solutions actually comply to the characteristics of the security solution for WMN (listed in Section 1.4). For example, very few solutions lead to the self-healing and self-organized WMN, primarily because of the lack of appropriate response mechanism to the detected anomalies and possible attacks in the network.
- A number of authentication mechanisms have been proposed for multi-hop wireless networks. However either the solutions incur unacceptable overheads to cater for mobility or the solutions are non-robust in an effort to accommodate the tradeoff between available resources and the achievable security level. Neither high mobility nor the resource limitation is a major design constraint for WMN. Therefore, the authentication mechanisms for WMN can be more robust with limited overhead and need to be redefined keeping in view the characteristics of WMN.
- Although efforts have been made to address the security issues originating from colluding malicious nodes that can launch the attacks like wormhole and black hole, no solution has successfully addressed the issue of colluding malicious nodes. The malicious and misbehaving nodes pose serious threats to WMN specifically if the network has to be self-healing and self-organized.
- No security mechanism has so far been proposed to address the security vulnerabilities in the joint channel assignment and routing algorithms for multi-radio multi-channel WMN. These algorithm are crucial for the performance of multi-radio multi-channel WMN and a security loophole in these algorithms can lead to severely degraded performance and, in some cases, the complete Denial-of-Service.
- IEEE 802.11i, the standard for security in wireless networks needs to address the issues identified in Section 1.6 before it can be integrated into IEEE 802.11s (draft standard

for WMN) as the security component.

## 1.8 Conclusion

In this chapter, we considered the security issues in wireless mesh networks that render these networks vulnerable to security attacks. Different security attacks on the MAC layer and network layer of wireless mesh networks have been considered in detail. Security mechanisms used to detect, prevent and counteract these attacks have been discussed briefly. The intrusion prevention mechanisms and the intrusion detection mechanisms used in various multi-hop wireless networks and applicable to wireless mesh networks have been considered. The IEEE 802.11i, standard for the security in wireless networks has been discussed in detail along with a note on the vulnerabilities rendering the protocol impractical for use in wireless mesh networks.

## References

- [1] Ashish Raniwala, Kartik Gopalan, Tzi-cker Chiueh. *Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks*. In ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), April 2004
- [2] Ashish Raniwala, Tzi-cker Chiueh. *Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network*. In proceedings of IEEE InfoCom. March 2005
- [3] Murali Kodialam, Thyaga Nandagopal. *Characterizing the capacity region in multi-radio multi-channel wireless mesh networks*. In proceedings of Mobile Computing and Networking. August 2005
- [4] Mansoor Alicherry, Randeep Bhatia, Li (Erran) Li. *Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks*. In proceedings of Mobile Computing and Networking. August 2005
- [5] Krishna N. Ramachandran, Elizabeth M. Belding-Royer, Kevin C. Almeroth and Milind

- M. Buddhikot. *Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks*. In Proceedings of IEEE Infocom 2006, April 2006.
- [6] P. Papadimitratos and Z. Haas. *Secure routing for mobile ad hoc networks*. in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.
- [7] Manel Guerrero Zapata and N. Asokan. *Securing Ad Hoc Routing Protocols*. In Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), September 2002.
- [8] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth Belding-Royer. *A Secure Routing Protocol for Ad hoc Networks*. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP '02), November 2002.
- [9] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. *Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks*. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pages 12-23, September 2002.
- [10] Huaizhi Li, Mukesh Singhal. *A Secure Routing Protocol for Wireless Ad Hoc Networks*. Proceedings of the 39th Hawaii International Conference on System Sciences, January 2006.
- [11] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. *Rushing attacks and defense in wireless ad hoc network routing protocols*. In Proceedings of the 2003 ACM workshop on Wireless security (WiSe 2003), in conjunction with MobiCom, pages 30-40, September 2003.
- [12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. *Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*. In Proceedings of IEEE INFOCOM 2003, April 2003.
- [13] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, Kendall E. Nygard. *Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks*. International Conference on Wireless Networks, pages 570-575, June 2003.
- [14] W. Xu, W. Trappe, Y. Zhang and T. Wood. *The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks*. In Proceedings of ACM MOBIHOC, 2005.
- [15] J. Pollastre, J. Hill and D. Culler. *Versatile Low Power Media Access for Wireless Sensor Networks*. In Proceedings of ACM Sensys 2004.

- [16] Y. Law, L. Hoesel, J. Doumen, P. Hartel and P. Havinga. *Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols*. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005).
- [17] T. Brown, J. James and A. Sethi. *Jamming and Sensing of Encrypted Wireless Ad Hoc Networks*. In Proceedings of ACM MOBIHOC, May 2006.
- [18] Arunesh Mishra, William A. Arbaugh, *An Initial Security Analysis of the IEEE 802.1X Standard*, Technical report, university of Marryland. February 2002.
- [19] Al-Shurman, M., Yoo, S., and Park, S. *Black hole attack in mobile Ad Hoc networks*. In Proceedings of the 42nd Annual Southeast Regional Conference. Huntsville, Alabama, April 2004.
- [20] Newsome, J.; Shi, E.; Song, D.; Perrig, A., *The Sybil attack in sensor networks: analysis and defenses*, Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pages 259- 268, April 2004.
- [21] Anjum Naveed and Salil S, Kanhere. *Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks*. To appear in Proceedings of IEEE GLOBECOM, November 2006.
- [22] S. Zhong, L.E. Li, Y.G. Liu and Y.R. Yang, *On Designing Incentive-Compatible Routing and Forwarding Protocols in Wireless Ad-Hoc Networks: An Integrated Approach using Game Theoretical and Cryptographic Techniques*. in Proceedings of IEEE MOBICOM, pages 117-131, August 2005.
- [23] N.B. Salem, L. Buttyan, J.-P. Hubaux, M. Jakobsson, *A Charging and Rewarding Scheme for Packet Forwarding in Multi-Hop Cellular Networks*. In Proceedings of IEEE MobiHoc, pages 1324, June 2003.
- [24] Y. Liu, H. Man and C. Comaniciu, *A Game Theoretic Approach to Efficient Mixed Strategies for Intrusion Detection*, to appear in IEEE International Conference on Communications (ICC) 2006.
- [25] Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P. S. Rocha, Antonio A. F. Loureiro, Linnyer B. Ruiz, Hao Chi Wong. *Decentralized intrusion detection in wireless sensor networks*, In Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks (Q2SWinet 2005), pages 16-23, October 2005.

- [26] Yi-an Huang, Wei Fan, Wenke Lee, Philip S. Yu. *Cross-feature analysis for detecting ad-hoc routing anomalies*. Proceedings. 23rd International Conference on Distributed Computing Systems, Pages: 478-487, May 2003.
- [27] Yi-an Huang, Wenke Lee. *A cooperative intrusion detection system for ad hoc networks*. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Pages: 135 - 147, October 2003.
- [28] Hao Yang, Shu. J, Xiaoqiao Meng, Songwu Lu. *SCAN: self-organized network-layer security in mobile ad hoc networks*, Appears in: IEEE Journal on Selected Areas in Communications, Volume: 24, Issue: 2, pages 261- 273, February 2006.
- [29] Security Architecture for Open Systems Interconnection for CCITT Applications, *ITU-T Recommendation X.800*, March 1991.
- [30] IEEE Std. 802.11i-2004, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements*. July, 2004. <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>.
- [31] Hamdy S. Soliman, Mohammed Omari. *Application of synchronous dynamic encryption system in mobile wireless domains*. In Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks (Q2SWinet '05), Pages 24-30, October 2005.
- [32] Kui Ren, Wenjing Lou, Yanchao Zhang. *LEDS: Providing Location-aware End-to-End Data Security in Wireless Sensor Networks*. In proceedings of IEEE International Conference on Computer Communication (INFOCOM'06), April 2006.
- [33] IEEE Std. 802.1X-2004, *IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control* June, 2001. <http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>
- [34] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., *Extensible Authentication Protocol (EAP)*, RFC 3748, June 2004.
- [35] C. Rigney, S. Willens, A. Rubens, W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, RFC 2865, June 2000.
- [36] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, *Diameter Base Protocol*, RFC 3588, September 2003.
- [37] D. Whiting, R. Housley, N. Ferguson, *Counter with CBC-MAC (CCM)*, RFC 3610,

September 2003.

- [38] Keoh, S. L. and Lupu, E. 2002. Towards flexible credential verification in mobile ad-hoc networks. In Proceedings of the Second ACM international Workshop on Principles of Mobile Computing Toulouse, France, October 2002. POMC '02.
- [39] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for MANET," in Proc. IEEE ICNP, 2001, pp. 251-260.
- [40] M. Junaid , Muid Mufti, M.Umar Ilyas, *Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol*, Transections on Engineering, Computing and Technology V11, February 2006.
- [41] Aboudagga, N., Refaei, M. T., Eltoweissy, M., DaSilva, L. A., and Quisquater, J. 2005. Authentication protocols for ad hoc networks: taxonomy and research issues. In Proceedings of the 1st ACM international Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05). Montreal, Quebec, Canada, October 2005.
- [42] Hongmei Deng; Mukherjee, A.; Agrawal, D.P., *Threshold and identity-based key management and authentication for wireless ad hoc networks*, In proceedings of International Conference on Information Technology: Coding and Computing (ITCC 2004). pages 107- 111 Vol.1, April 2004.
- [43] Lim, Y.-X.; Yer, T.S.; Levine, J.; Owen, H.L., *Wireless intrusion detection and response*, Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society , pages 68-75, June 2003.
- [44] Changhua He, John C Mitchell, *Analysis of the 802.11i 4-Way Handshake*, WiSE04, Philadelphia, Pennsylvania, USA, October 2004.
- [45] Arunesh Mishra, William A. Arbaugh, *An Initial Security Analysis of the IEEE 802.1X Standard*, Technical Report CS-TR-4328, Department of Computer Science, University of Marryland. February 2002. <https://drum.umd.edu/dspace/handle/1903/1179?mode=full>



M replies positively to every Route Request

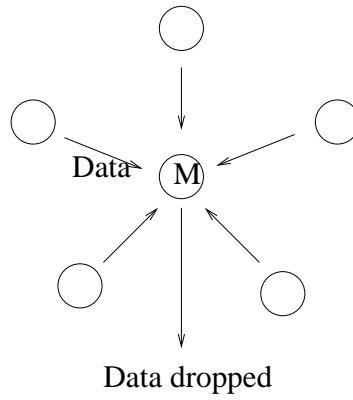


Figure 1.4: Black hole attack, Node M replies positively to every Route Request. Consequently all data is forwarded to the node which then drops the data.

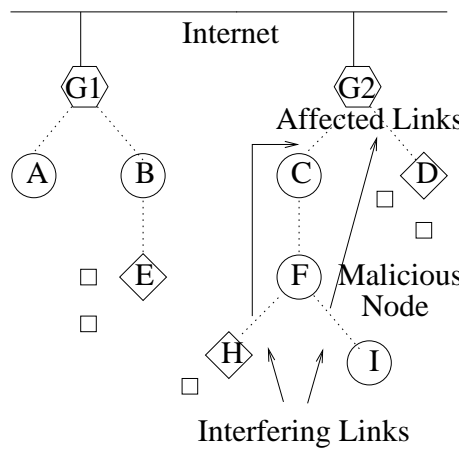


Figure 1.5: NEPA Attack. Assuming the node F is within interference domain of node G.

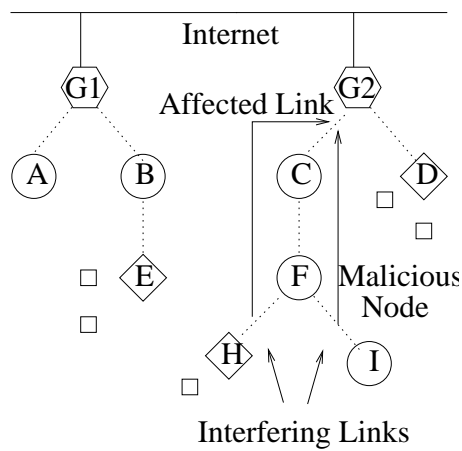


Figure 1.6: CEPA Attack. Assuming the node F is within interference domain of node G.

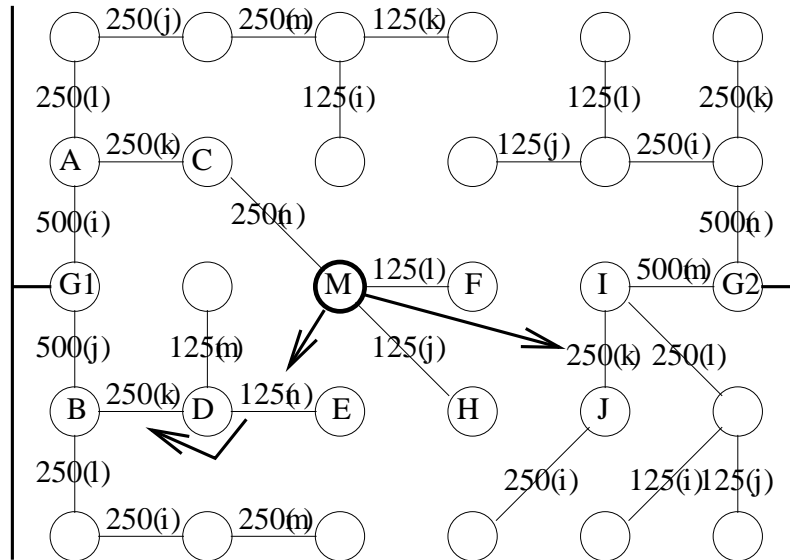


Figure 1.7: Example WMN with routers physically arranged in grid topology. G1 and G2 are gateways connected to wired network. Edges show routing topology and labels along edges are [bandwidth in kbps(channel)]. For simplicity,  $k + 1$ -hop neighbors include immediate physical neighbors only. Arrows show propagation of ripple effect attack from compromised node M.

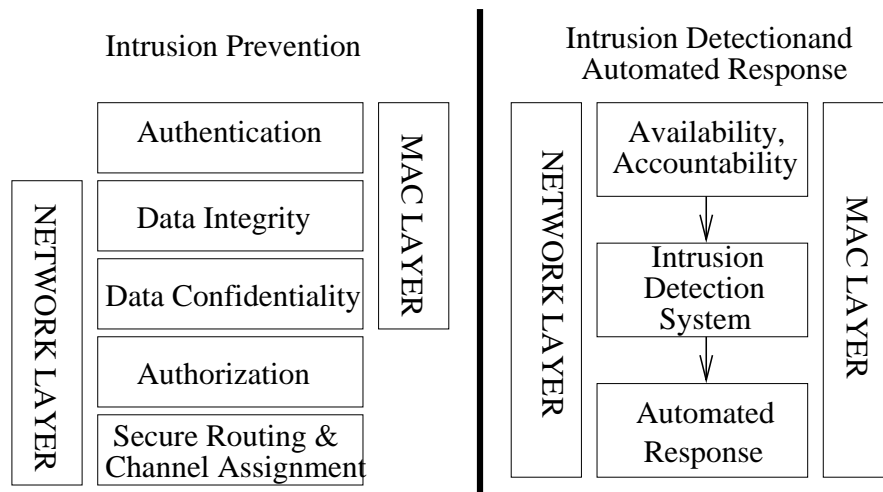


Figure 1.8: Security Model for Wireless Mesh Networks.

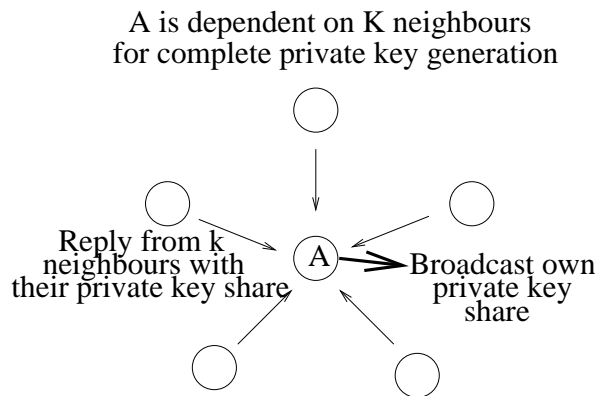


Figure 1.9: Neighbour collaboration for private key generation in Wireless Mesh Networks.

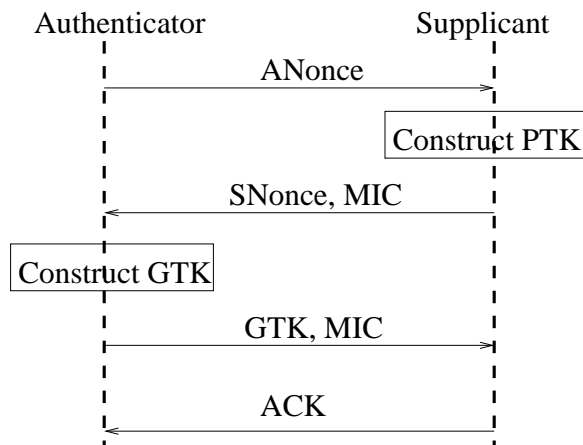


Figure 1.10: Four-way handshake

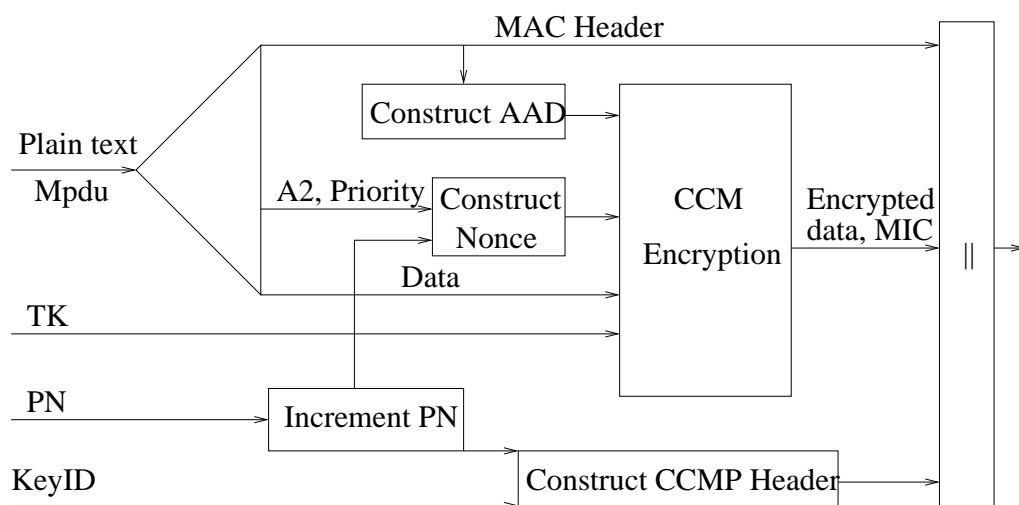


Figure 1.11: CCMP encryption process and encrypted frame generation.

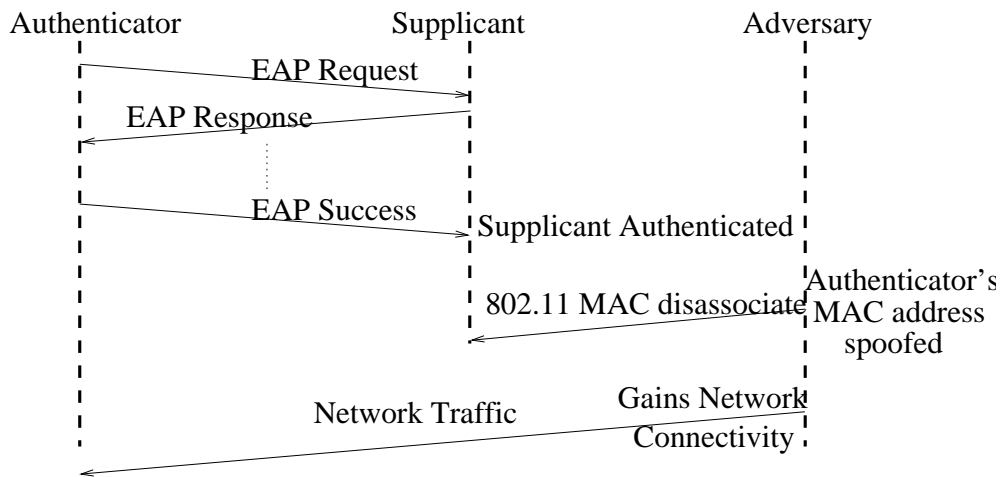


Figure 1.12: Session hijacking attack on 802.1X authentication mechanism

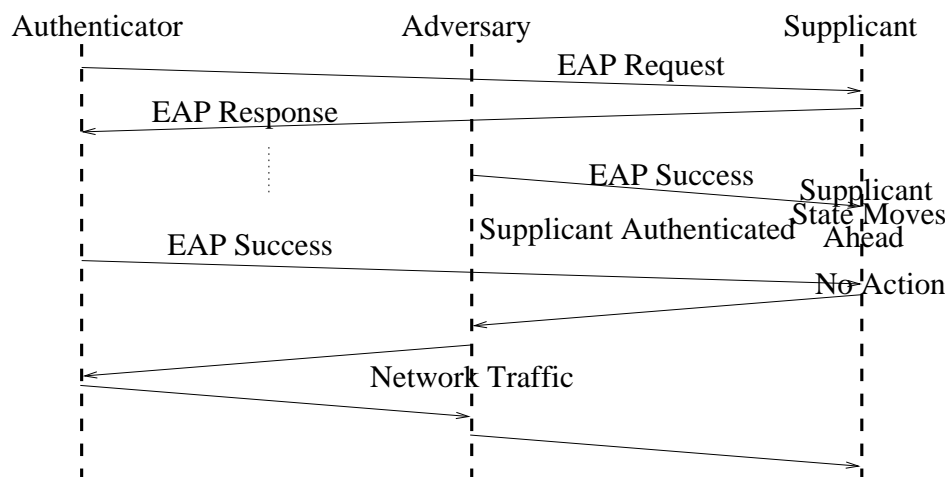
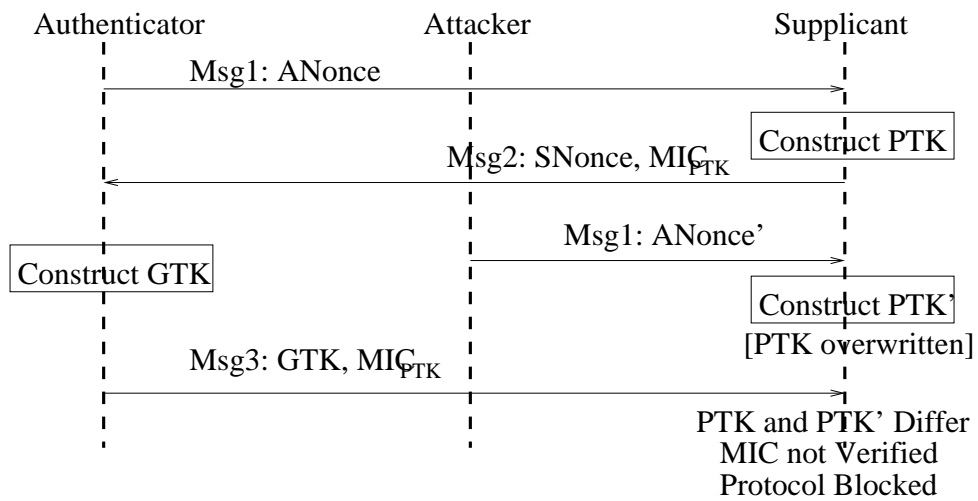


Figure 1.13: Man-in-the-middle attack on 802.1X authentication mechanism



(Attacker sends messages with spoofed MAC address of Authenticator)

Figure 1.14: Denial-of-Service attack on four-way handshake