Applications of Cryptography and Network Security

Stephen Mason

Applications of Cryptography and Network Security

Edited by **Stephen Mason**

CLANRYE INTERNATIONAL

New Jersey

Published by Clanrye International,
55 Van Reypen Street,
Jersey City, NJ 07306, USA
www.clanryeinternational.com

Applications of Cryptography and Network Security
Edited by Stephen Mason

International Standard Book Number: 978-1-63240-065-9 (Hardback)

Printed in China.

Applications of Cryptography and Network Security

Preface

Cryptography is the essential and efficient ingredient to the recipe of security solutions. With the arrival of new age communication systems and high speed networks in the future, cryptography will have a key role to play. This book talks about the crucial security challenges that the computing world is facing today and also discusses several techniques to fight against such attacks. The chapters in this book discuss various facets of cryptography and their applications. It will cater to the needs of researchers, engineers, graduates and PhD students working in this field. It will also be beneficial to teachers at universities and colleges as a reference.

This book unites the global concepts and researches in an organized manner for a comprehensive understanding of the subject. It is a ripe text for all researchers, students, scientists or anyone else who is interested in acquiring a better knowledge of this dynamic field.

I extend my sincere thanks to the contributors for such eloquent research chapters. Finally, I thank my family for being a source of support and help.

Editor

Contents

Part 1

Security and Privacy in Computing and Communication Networks

1

Secure and Privacy-Preserving Authentication Protocols for Wireless Mesh Networks

Jaydip Sen
Innovation Lab, Tata Consultancy Services Ltd.
India

1. Introduction

Wireless mesh networks (WMNs) have emerged as a promising concept to meet the challenges in next-generation wireless networks such as providing flexible, adaptive, and reconfigurable architecture while offering cost-effective solutions to service providers (Akyildiz et al., 2005). WMNs are multi-hop networks consisting of *mesh routers* (MRs), which form wireless mesh backbones and *mesh clients* (MCs). The mesh routers provide a rich radio mesh connectivity which significantly reduces the up-front deployment cost of the network. Mesh routers are typically stationary and do not have power constraints. However, the clients are mobile and energy-constrained. Some mesh routers are designated as gateway routers which are connected to the Internet through a wired backbone. A gateway router provides access to conventional clients and interconnects ad hoc, sensor, cellular, and other networks to the Internet. The gateway routers are also referred to as the *Internet gateways* (IGWs). A mesh network can provide multi-hop communication paths between wireless clients, thereby serving as a community network, or can provide multi-hop paths between the client and the gateway router, thereby providing broadband Internet access to the clients.

As WMNs become an increasingly popular replacement technology for last-mile connectivity to the home networking, community and neighborhood networking, it is imperative to design efficient and secure communication protocols for these networks. However, several vulnerabilities exist in the current protocols of WMNs. These security loopholes can be exploited by potential attackers to launch attack on WMNs. Absence of a central point of administration makes securing WMNs even more challenging. Security is, therefore, an issue which is of prime importance in WMNs (Sen, 2011). Since in a WMN, traffic from the end users is relayed via multiple wireless mesh routers, preserving privacy of the user data is also a critical requirement (Wu et al., 2006a). Some of the existing security and privacy protection protocols for WMNs are based on the trust and reputation of the network entities (Sen, 2010a; Sen, 2010b). However, many of these schemes are primarily designed for *mobile ad hoc networks* (MANETs) (Sen, 2006; Sen, 2010c), and hence these protocols do not perform well in large-scale hybrid WMN environments.

The broadcast nature of transmission and the dependency on the intermediate nodes for multi-hop communications lead to several security vulnerabilities in WMNs. The attacks can be external as well as internal in nature. External attacks are launched by intruders who are

not authorized users of the network. For example, an intruding node may eavesdrop on the packets and replay those packets at a later point of time to gain access to the network resources. On the other hand, the internal attacks are launched by the nodes that are part of the WMN. On example of such attack is an intermediate node dropping packets which it was supposed to forward. To prevent external attacks in vulnerable networks such as WMNs, strong authentication and access control mechanisms should be in place for practical deployment and use of WMNs. A secure authentication should enable two communicating entities (either a pair of MC and MR or a pair of MCs) to validate the authenticity of each other and generate the shared common session keys which can be used in cryptographic algorithms for enforcing message confidentiality and integrity. As in other wireless networks, a weak authentication scheme can easily be compromised due to several reasons such as distributed network architecture, the broadcast nature of the wireless medium, and dynamic network topology (Akyildiz et al., 2005). Moreover, the behavior of an MC or MR can be easily monitored or traced in a WMN by adversaries due to the use of wireless channel, multi-hop connection through third parties, and converged traffic pattern traversing through the IGW nodes. Under such scenario, it is imperative to hide an active node that connects to an IGW by making it anonymous. Since on the Internet side traditional anonymous routing approaches are not implemented, or may be compromised by strong attackers such protections are extremely critical (X. Wu & Li, 2006).

This chapter presents a comprehensive discussion on the current authentication and privacy protection schemes for WMN. In addition, it proposes a novel security protocol for node authentication and message confidentiality and an anonymization scheme for privacy protection of users in WMNs.

The rest of this chapter is organized as follows. Section 2 discusses the issues related to access control and authentication in WMNs. Various security vulnerabilities in the authentication and access control mechanisms for WMNs are first presented and then a list of requirements (i.e. properties) of a secure authentication scheme in an open and large-scale, hybrid WMN are discussed. Section 3 highlights the importance of the protection user privacy in WMNs. Section 4 presents a state of the art survey on the current authentication and privacy protection schemes for WMNs. Each of the schemes is discussed with respect to its applicability, performance efficiency and shortcomings. Section 5 presents the details of a hierarchical architecture of a WMN and the assumptions made for the design of a secure and anonymous authentication protocol for WMNs. Section 6 describes the proposed key management scheme for secure authentication. Section 7 discusses the proposed privacy protection algorithm which ensures user anonymity. Section 8 presents some performance results of the proposed scheme. Section 9 concludes the chapter while highlighting some future direction of research in the field of secure authentication in WMNs.

2. Access control and authentication in WMNs

Authentication and authorization is the first step towards prevention of fraudulent accesses by unauthorized users in a network. Authentication ensures that an MC and the corresponding MR can mutually validate their credentials with each other before the MC is allowed to access the network services. In this section, we first present various attacks in WMNs that can be launched on the authentication services and then enumerate the requirements for authentication under various scenarios.

2.1 Security vulnerabilities in authentication schemes

Several vulnerabilities exist in different protocols for WMNs. These vulnerabilities can be suitably exploited by potential attackers to degrade the network performance (Sen, 2011). The nodes in a WMN depend on the cooperation of other nodes in the network for their successful operations. Consequently, the *medium access control* (MAC) layer and the network layer protocols for these networks usually assume that the participating nodes are honest and well-behaving with no malicious or dishonest intentions. In practice, however, some nodes in a WMN may behave in a selfish manner or may be compromised by malicious users. The assumed trust (which in reality may not exist) and the lack of accountability due to the absence of a central point of administration make the MAC and the network layer protocols vulnerable to various types of attacks. In this sub-section, we present a comprehensive discussion on various types of attacks on the existing authentication schemes of WMNs. A detailed list various attacks on the different layers of WMN communication protocol stack can be found in (Sen, 2011; Yi et al., 2010).

There are several types of attacks that are related to authentication in WMNs. These attacks are: (i) unauthorized access, (ii) replay attack, (iii) spoofing attack, (iv) denial of service attack (DoS), (v) intentional collision of frames, (vi) pre-computation and partial matching attack, and (vi) compromised or forged MRs. These attacks are discussed in detail below.

Unauthorized access: in this attack, an unauthorized user gets access to the network services by masquerading a legitimate user.

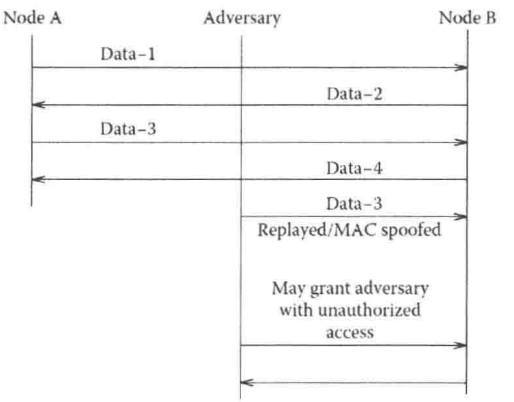

Fig. 1. Illustration of MAC spoofing and replay attacks [Source: (Sen, 2011)]

Replay attack: the replay attack is a type of *man-in-the-middle* attack (Mishra & Arbaugh, 2002) that can be launched by external as well as internal nodes. An external malicious node can eavesdrop on the broadcast communication between two nodes (*A* and *B*) in the network as shown in Fig. 1. It can then transmit legitimate messages at a later point of time to gain access to the network resources. Generally, the authentication information is replayed where the attacker deceives a node (node *B* in Fig. 1) to believe that the attacker is a legitimate node (node *A* in Fig. 1). 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 unauthorized access to the network resources.

Spoof attack: spoofing is the act of forging a legitimate MAC or IP address. IP spoofing is quite common in multi-hop communications in WMNs. In IP spoofing attack, an adversary inserts a false source address (or the address of a legitimate node) from the packets forwarded by it. Using such a spoofed address, the malicious attacker can intercept a termination request and hijack a session. In MAC address spoofing, the attacker modifies the MAC address in transmitted frames from a legitimate node. MAC address spoofing enables the attacker to evade *intrusion detection systems* (IDSs) that may be in place.

DoS attack: in this attack, a malicious attacker sends a flood of packets to an MR thereby making a buffer overflow in the router. Another well-known security flaw can be exploited by an attacker. In this attack, a malicious attacker can send false termination messages on behalf of a legitimate MC thereby preventing a legitimate user from accessing network services.

Intentional collision of frames: a collision occurs when two nodes attempt to transmit on the same frequency simultaneously (Wood & Stankovic, 2002). When frames collide, they are discarded and need to be retransmitted. An adversary may strategically cause collisions in specific packets such as acknowledgment (ACK) control messages. A possible result of such collision is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions. Repeated collisions can also be used by an attacker to cause resource exhaustion. For example, a naïve MAC layer implementation may continuously attempt to retransmit the corrupted packets. Unless these retransmissions are detected early, the energy levels of the nodes would be exhausted quickly. An attacker may cause unfairness by intermittently using the MAC layer attacks. In this case, the adversary causes degradation of real-time applications running on other nodes by intermittently disrupting their frame transmissions.

Pre-computation and partial matching attack: unlike the attacks mentioned above, where the 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 the MAC layer to secure the communication. In a pre-computation attack, or *time memory trade-off* (TMTO) attack, the attacker computes a large amount of information (e.g., key, plaintext, and the corresponding ciphertext) 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 (ciphertext, plaintext) pairs, which in turn decreases the encryption key strength, and improves the chances of success of the brute force mechanisms. Partial matching attacks exploit the weak implementations of encryption algorithms. For example, the 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 that exploits the vulnerabilities in IEEE802.1X. DoS attacks are possible on the four-way handshake procedure in IEEE802.11i.

Compromised or Forged MR: an attacker may be able to compromise one or more MRs in a network by physical tampering or logical break-in. The adversary may also introduce rogue MRs to launch various types of attacks. The fake or compromised MRs may be used to

attack the wireless link thereby implementing attacks such as: passive eavesdropping, jamming, replay and false message injection, traffic analysis etc. The attacker may also advertise itself as a genuine MR by forging duplicate beacons procured by eavesdropping on genuine MRs in the network. When an MC receives these beacon messages, it assumes that it is within the radio coverage of a genuine MR, and initiates a registration procedure. The false MR now can extract the secret credentials of the MC and can launch spoof attack on the network. This attack is possible in protocols which require an MC to be authenticated by and MR but not the vice versa (He et al., 2011).

2.2 Requirements for authentication in WMNs

On the basis of whether a central authentication server is available, there are two types of implementations of access control enforcements in WMNs: (i) centralized access control and (ii) distributed access control. For both these approaches, the access control policies should be implemented at the border of the mesh network. In the distributed access control, the access points could act as the distributed authentication servers. The authentication could also be performed in three different places:

- A remote central authentication center
- Local entities such as IGWs or MRs that play the role of an authentication server
- Local MRs

The main benefit of central authentication server is the ease of management and maintenance. However, this approach suffers from the drawback of having a single point of failure. Due to higher *round trip time* (RTT) and authentication delay, a centralized authentication scheme in a multi-hop WMN is not desirable. Instead, authentication protocols are implemented in local nodes such as IGW or MRs. For ensuring higher level of availability of the network services, the authentication power is delegated to a group of MRs in order to avoid single point of failure.

The objective of an authentication system is to guarantee that only the legitimate users have access to the network services. Any pair of network entities in a WMN (e.g., IGW, MR, and MC) may need to mutually authenticate if required. An MR and MC should be able to mutually authenticate each other to prevent unauthorized network access and other attacks. The MCs and MRs should be able to establish a shared pair-wise session key to encrypt messages. The protocol should have robust key generation, distribution and revocation procedures.

Several requirements have been identified in (Buttyan et al., 2010) for authentication mechanisms between MC and MRs in a WMN. These requirements are summarized below:

- *Authentication should be fast enough to support user mobility.* In order to maintain the *quality of service* (QoS) of user applications on mobile MCs, the authentication process should be fast. Also, the re-authentication delays should be within the acceptable limit of handoff delay.
- *MCs and MRs should be able to authenticate themselves mutually.* During the authentication process, the MR authenticates the MC, but the MR also should prove its authenticity to the MC.
- *Authentication process should be resistant to DoS attacks.* Since a successful attack against the central authentication server will lead to a complete compromise of the security system in the network, the authentication process should be robust.

- *Authentication protocols should be compatible with standards.* In a multi-operator environment, it is mandatory that the authentication protocols are standardized so that an MC of one vendor should be able to authenticate with the MR of a different network operator.
- *Authentication protocols should be scalable.* Since the mesh networks have large number of MCs, MRs and IGWs, the authentication protocol should be scalable and must not degrade in performance as the network size increases.

The mutual authentication protocols for MCs and MRs must use several keys for encrypting the credentials. The connection key management should satisfy the following requirements.

- *The connection keys should not reveal long term keys.* The connection keys that the MRs obtain during the authentication of the MCs should not reveal any long-term authentication keys. This requirement must hold because in the multi-operator environment, the MCs may associate to MRs operated by foreign operators.
- *The connection keys should be independent of each other.* As the neighboring MRs may not fully trust each other in a multi-operator environment, the authentication and key generation mechanism have to prevent an MR from deriving connection keys that are used at another MR.
- *The connection keys must be fresh in each session.* It must be ensured that the connection key derived during the authentication protocol for both participants (MC and MR) is fresh.

3. User privacy requirement in WMNs

Privacy provision is an important issue to be considered for WMN deployment. However, privacy is difficult to achieve even if messages are protected, as there are no security solutions or mechanisms which can guarantee that data is not revealed by the authorized parties themselves (Moustafa, 2007). Thus, it is important that complementary solutions are in place. Moreover, communication privacy cannot not be assured with message encryption since the attackers can still observe who is communicating with whom as well as the frequency and duration of the communication sessions. This makes personal information susceptible to disclosure and subsequent misuse even when encryption mechanisms are in place. Furthermore, users in WMNs can be easily monitored or traced with regard to their presence and location, which causes the exposure of their personal life. Unauthorized parties can get access to the location information about the MC's positions by observing their communications and traffic patterns. Consequently, there is a need to ensure location privacy in WMNs as well.

To control the usage of personal information and the disclosure of personal data, different types of information hiding mechanisms like anonymity, data masking etc should be implemented in WMN applications. The following approaches can be useful in information hiding, depending on what is needed to be protected:

- *Anonymity*: this is concerned with hiding the identity of the sender or receiver of the message or both of them. In fact, hiding the identity of both the sender and the receiver of the message can assure communication privacy. Thus, attackers monitoring the messages being communicated could not know who is communicating with whom, thus no personal information is disclosed.