ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Security Issues & Challenges in Wireless Mesh Networks

Umesh Kumar Singh
Institute of Computer Science
Vikram University Ujjain (M.P.) INDIA
umeshsingh@rediffmail.com

Shivlal Mewada*
Institute of Computer Science
Vikram University Ujjain (M.P.) INDIA
shiv.mewada@gmail.com

Abstract: Wireless Mesh Network (WMN) is a new wireless networking paradigm. Unlike traditional wireless networks, WMNs do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Wireless internet service providers are choosing WMNs to offer Internet connectivity, as it allows a fast, easy and inexpensive network deployment. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we describe the specifics of WMNs and we identify three primary network operations that need to be secured. We identify the new challenges and opportunities posed by this new networking environment and explore approaches to secure its communication.

Keywords: Wireless Mesh Networks, cellular networks, security, authentication

I. INTRODUCTION

All WMNs represent a new network concept and therefore introduce new security specifics. Here, we describe these specifics by giving an overview of the primary differences between WMNs and two well-established infrastructure based technologies: cellular networks and the Internet.

The major difference between WMNs and cellular networks - besides the use of different frequency bands (WMNs usually make use of unlicensed frequencies) - concerns the network configuration: In cellular networks, a given area is divided into cells and each cell is under the control of a base station. Each base station handles a certain number of mobile clients that are in its immediate vicinity (i.e., communication between the mobile clients and the base station is single-hop) and it plays an important role in the functioning of the cellular network; the entity that plays an equivalent role in WMNs would be the Wireless Host Spots [1].

However, whereas all the security aspects can be successfully handled by the base station in cellular networks, it is risky to rely only on the Wireless Host Spots to secure a WMN, given that the communications in WMNs are multi-hop. Indeed, centralizing all security operations at the WHS would delay attack detection and treatment and therefore would give the adversary an undeniable advantage. Furthermore, multi-hopping makes routing in WMNs a very important and necessary functionality of the network; and like all critical operations, an adversary may be tempted to attack it. The routing mechanism must thus be secured.

Multi- hopping has also an important effect on the network utilization and performance. Indeed, if the WMN is not well-designed, a Transmit Access Points (TAPs) that is several hops away from the WHS would receive a much lower bandwidth share than a TAP that is next to it. This leads to severe unfairness problems, and even starvation [2]; it thus can be used by an adversary to disturb the functioning of the WMN.

In WMNs, the wireless TAPs play the role that is played, in the classic (wired) Internet, by the routers. Given that wireless communications are vulnerable to passive attacks such as eavesdropping, as well as to active attacks such as Denial of Service (DoS), WMNs are subject to all these attacks whose effects are amplified by the multi-hop aspect of the communications.

Another primary difference between the Internet and WMNs is that, unlike Internet routers, the TAPs are not physically protected. Indeed, they are most often in locations that are accessible to potential adversaries, e.g., deployed on rooftops or attached to streetlights. The absence of physical protection of the devices makes WMNs vulnerable to some serious attacks. Indeed, one very important requirement regarding the Transmit Access Points - for the concept of mesh networks to remain economically viable - is their low cost that excludes the possibility of strong hardware protection of the devices (e.g., detection of pressure, voltage, or temperature changes) [1,3]. Therefore, attacks such as tampering, capture or replication of Transmit Access Point s are possible and even easy to perform.

This brief analysis of the characteristics of WMNs clearly shows that, compared with other networking technologies, the new security challenges are mainly due to the multi-hop wireless communications and by the fact that the Transmit Access Points are not physically protected. Multi-hopping delays the detection and treatment of the attacks, makes routing a critical network service and may lead to severe unfairness between the TAPs, whereas the physical exposure of the TAPs allows an adversary to capture, clone or tamper with these devices.

II. SECURITY MANGAGEMENT

Security is critical in the process of deploying and management of Wireless Mesh Networks (WMNs). In WMNs, like in MANETs (Mobile Ad Hoc networks), security is easy to compromise due to specific characteristics of these networks:

a. There is a shared wireless medium among the network nodes; this means that channels are vulnerable
b. The topology of the network changes dynamically making it more difficult to trace malicious actions

The possible attacks may occur at routing protocol or MAC protocol levels. Routing attacks include: advertising routing updated for DSR (Dynamic Source Routing) and AODV (Ad Hoc On Demand Vector) protocols, packet forwarding (which may act without changing the routing tables, but still leading packets on the routing path to a different destination), impersonating a legitimate node and misbehaving, or creating a wormhole and shortcutting the normal flows.

Naouel Ben Salem presents in [1], starting from a simplified view of a WMN, three primary security operations, namely: detecting corrupt TAPs, securing multihop routing and assuring fairness. The approach draws from the security paradigm, and adds to it the challenges encountered due to the specific characteristics of WMNs: multihop network, power constraints and mobility. Several verification scenarios are discussed: authentication of a mobile client (MC) in relation to a TAP, mutual authentication of TAPs and/or the WHS, and integrity verification. Symmetric key cryptography is preferred over asymmetric cryptography on time and complexity reasons, and a solution for message authentication, based on Message Authentication Codes (MACs), is presented. Based on these assumptions, counter measures are enumerated for attacks mainly grouped according to their target actions: corrupting TAPs, Multihop routing attacks, and attacks that disturb the fairness in the network. The architecture of a WMN is a little simplified, as it does not consider the possibility of multiple routers with gateway functions (WHS) for "internet" access, and thus it does not catch more complex interactions going on in the network. Finally, an example is given, of vehicular networks, where the concept of WMNs is not fully (correctly) exploited, by fixing WHS on telephone posts along-side the road, and considering vehicles, mobile TAPs. This would have better fit the model if the vehicles had been mobile clients switching from a static TAP to another as they move along the road.

III. SECURITY CHALLENGES OF WMNS

Certain verifications need to be performed as related to interaction between mobile clients and Wireless Access Points (also known as TAPs, or wireless mesh routers):

a. Mobile Client authentication; this can be anything of the already existent techniques (drawn from wired networks, or from mobile telephony):
   i. Use of predefined shared secret
   ii. Employment roaming system
   iii. or of a temporary billing account
   iv. Public key cryptography primitives – unsuitable because not energy efficient
   v. Attacker can continuously ask the MC to compute or verify signatures –> MC battery drainage

Public key cryptography primitives for this case are unsuitable because they are not energy efficient. Since a mobile node is power sensible, an attacker can exploit this and can continuously ask the mobile node to compute or verify signatures. This, in time will lead mobile client battery drainage, and consequently will take the node out of the network.

b. Mutual authentication of network nodes. This is done in two phases:

At initialization phase, when WMN is first deployed (or re-initialization–if reconfiguration of the network needed). Asymmetric key cryptography can be performed here since TAPs (Wireless Access Points) and WHS (Wireless Hot Spots, also known as Wireless Gateways) are energy rich. For this to be done, the managing operator assigns a certified public/private key pair to TAPs and WHS. The mobile client can use the TAP's certified public key for authentication during session establishment.

During session established by the MC Public key cryptography to authenticate the sender/receiver for every packet is a heavy process and is not suitable for Wireless Mesh network architecture. The alternative is symmetric key cryptography. This is employed by using session keys or long-term shared keys that were originally loaded into the nodes. Message Authentication Codes (MAC) is then computed for messages between intermediate TAPs on the basis of symmetric keys predefined for each neighboring TAPs pair

c. Integrity verification .This is done either end-to-end, or at each intermediate TAP, or both. A solution could be for nodes to establish a symmetric key with the MC (mobile client). The message is protected by the MC using the MAC scheme as defined in [1]

A. Detection of Corrupt TAPs:

Physical capture of a TAP is not necessary. Distant hacking can be employed for this. The WHS (Wireless Hot Spots or Wireless Gateway) is assumed to be physically protected. Thus it can be used to handle/store critical cryptographic data (instead of the TAPs). Four main attacks can be performed on TAPs:

a. Simple removal/replacement of a TAP. This may be done to modify the topology of the network to the benefit of the adversary.
b. Access the internal state of the captured device without changing it. This is a passive attack and is done with the purpose of retrieving secret data (public/private key pair, symmetric keys shared with neighbouring TAPs or WHS) from the TAP. A solution to counteract this type of attack is periodic erasure and reprogramming of TAPs.
c. Modify the internal state of the TAP. The purpose of this attack can be to modify the routing algorithm with the final goal of changing the network topology. A combat solution is presented by Seshadri et al in [4].
d. Clone the captured device and install replicas in strategic places in the network. The purpose of this attack is to inject false data or disconnect parts of the WMN.

B. Secure Multi-hop Routing:

Due to the multi-hop nature of the WMNs, the routing mechanisms are essential to the smooth, effective running of the network. Compromising this area could seriously damage network performance. It is therefore of utmost importance that it is kept secure. Possible threats that a WMN can succumb to if its routing mechanisms are not secure:

a. Deteriorating performance of the network by increasing the length of communication paths between the WHS and the TAPs.

b. Isolation of a TAP which could inadvertently mean the isolation of a geographic region (which connects to the network by means of the isolated TAP).

c. Redirecting traffic through a particular TAP in order to monitor the traffic.Further methods for attacking the routing mechanisms by means of packet injection are:

d. Black hole - Creating forged packets to impersonate a valid mesh node simultaneously dropping packets (attracting packets is done by advertising routes as low-cost) [5].

e. Grey hole - Creating forged packets to (i) attack and selectively drop, routes or (ii) inspect network traffic.

f. Worm hole - Routing control messages and replaying them in different locations in the network to severely disrupt routing.

g. Route error injection - disrupting routing by injecting forged route error message in order to break mesh links.

The last attack (route error injection) in comparison to the other routing attacks has higher exploitability because it does not require detailed knowledge.

C. Vehicular networks:

So far, we have assumed the TAPs to be static. Vehicular networks represent a special case of WMNs that consists of a set of mobile TAPs (represented by the cars) and of roadside WHSs. The spectrum of applications offered by a vehicular network is wide ranging: It goes from safety related applications such as reporting important events (e.g., an accident) or traffic optimization through cooperative driving (e.g., deviate the traffic to avoid a traffic jam) to payment services (e.g., electronic toll collection) and location-based services (e.g., targeted marketing)[1].

D. ARSA:

Yanchao Zhang et al, in ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks, [5], presents an architecture which eliminates the need for establishing bilateral roaming agreements and real-time interactions between potentially numerous WMN operators. The architecture is based on the assumption that the Wireless Mesh Network operates under an operator control and replaces the home/foreign-domain model usually encountered in GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunication System) or Mobile IP networks which involves the existence of a home domain where a user is registered and account information is kept, and which is contacted by foreign domains every time authentication or payment settling is needed.

The paper is mainly focused on security issues relating to network access (as opposed to infrastructure security – believed to be taken care of by the operators, and application security – achieved via high-layer security mechanisms like IPSec) such as: router – client AKA, client – client AKA, location privacy, signaling authentication and service availability. It further explains how security is achieved for this using identity-based cryptography (IBC) as an alternative to certificate-based cryptography (CBC).

ARSA entitles the existence of brokers which issue universal *passes* to users, who then can roam freely in the domains of the WMN operators who have made agreements with brokers (far less in number then WMN operators). Authentication and key agreement (AKA) between a client and a WMN domain would then only involve a local interaction, which spares a lot of overhead.

The whole concept is built across trust domains, which, in ARSA, are managed by brokers or by WMN operators. These offer passes as follows:

a. router passes (R-Passes) are issued by a WMN operator to routers in its domain

b. client passes (C-Passes) are issued by a broker to registered clients

c. temporary client passes (T-Passes) are issued by a WMN operator to clients roaming in its domain

IV. SECURITY ENHANCEMENTS

The presented authentication and key agreement procedure makes client and impersonation attacks difficult to realize. There are however other issues which should be taken into consideration for proper security mechanisms: location privacy, bogus beacon flooding or denial of access attacks and bandwidth exhaustion attacks.

A feasible attack is flooding the mesh with bogus beacons. This is called in [5], the bogus-beacon flooding attack. The fact that the beacon sending interval is very short entails a great burden on the mesh clients (as they have to do a verification of the validity of the pass the router is advertising). The way to go past this is based on a hash-chain technique, to reduce the computational load of both routers and clients (signature operations are replaced with hash operations which are some orders of magnitude faster). A router will generate a signature at the start of each super beacon interval (which is an integer number of times bigger than the normal beacon interval). Thus, the clients check signature only once per super beacon interval.

The reverse way attack is sending a large number of bogus authentication responses to a mesh router to exhaust its resources, thus realizing a denial-of-access attack (DoA). The router defends against such an attack by using a client-puzzle scheme, in which whenever he detects a sign of attack (a large number of authentication responses suddenly received), it requires the solution of a cryptographic puzzle attacked to each authentication response. It is feasible to implement such a scheme, since the solution space is hard and thus an attacker (unless he has abundant resources) will have to slow down the bogus message rate according to the rate at which he finds the solutions. On the other hand, verification of the solution is trivial, thus keeping the router at an acceptable computation burden. The back draw of the scheme is that is increases the computational load on legitimate clients as well, but they will still be able to obtain network access.

In a bandwidth exhaustion attack, an attacker continuously sends data packets destined for a mesh router at a high rate. Legitimate clients waste plenty of resources to forward the attacker’s packets. To fight against this attack, pairwise shared-keys have to be established between all clients and the router (to which the attacking packets are forwarded). Thus, an attacker would have to attach keyed Message Integrity Checks (MICs) computed with the shared key he holds with nodes on the route, with each of these nodes on the route. Each intermediate client can check the packet before forwarding it to the next hop. This way, an unauthenticated client will not be able to send his packet in multi-hops to the router.

If the attacker is a legitimate user (each forwarding node, including the router, authenticates him), the router can slow him down by economic means. Here, the attacker can choose to avoid the router, by attaching incorrect MICs only for the last few hops. Packets will never reach the router, and the attacker manages to take a lot of the bandwidth of some of the forwarding clients. An extra-security protection for this case would be the client-puzzle approach on top.

V. CONCLUSIONS

Wireless mesh networks represent an easy and inexpensive result to extend the coverage of a Wireless Hot Spots. However, the deployment of such networks is slowed down by the lack of security guarantees. In this paper, we have analyzed the characteristics of wireless mesh networks and have deduced three primary network operations that need to be secured: Transmit Access Points secure routing protocol, a proper fairness metric in wireless mesh networks.

VI. REFERENCE

[1]. Naouel Ben Salem and Jean-Pierre Hubaux, EPFL,” securing wireless mesh networks”, Proc. Wireless Communications , vol. 13, no. 2, pp. 50-55, April 2006.

[2]. I. Akyildiz and X. Wang, “A survey on wireless mesh networks,” IEEE Communications Magazine, vol. 43, no. 9, pp. 23–30, 2005.

[3]. R. Anderson and M. Kuhn. “Tamper Resistance - a Cautionary Note”. In The Second USENIX Workshop on Electronic Commerce Proceedings, 1996.

[4]. A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. Swatt: Software-based attestation for embedded devices. In In IEEE Symposium on Security and Privacy, 2004.

[5]. Y. Zhang, Y.; Fang. ARSA: An attack-resilient security architecture for multihop wireless mesh networks. In IEEE Journal on Selected Areas in Communications, volume 24, pages 1916–1928, Oct. 2006.