World Journal of Research and Review (WJRR)
ISSN:2455-3956, Volume-3, Issue-2, August 2016 Pages 78-81

Wireless LAN Security: The IEEE 802.11 Risks and Technical Challenges

Amit Mishra, Dangana Muhammad, Joseph Elijah, Dinesh Kumar

Abstract— **Wireless local area networks (LANs) are playing a major role in the information technology revolution. They have found their way into a wide variety of markets including financial sectors, corporations, health care, and education.The rapid deployment of wireless LANs is testimony to the inherent benefits of this technology. Unfortunately, most wireless deployments are, at this time, fundamentally insecure. This is not an exaggeration. It is an accurate assessment of the reality of the current state of the security of wireless 802.11-based environments.Because of its transmission characteristic, many security problems have set in. This paper aims to introduce the security mechanism of the wireless LAN and points out the shortcoming of it.**

Index Terms—**About four key words or phrases in alphabetical order, separated by commas.**

I. Introduction

The deployment of Wireless Local Area Networks (WLANs) has rapidly grown over the last years [3]. Wireless LANs are easy to install even by computer-illiterate persons [1, 2] and they can be utilized in places where traditional Ethernet wire cannot reach. In the simplest of terms, a wireless local-area network (WLAN) does exactly what the name implies: it provides all the features and benefits of traditional LAN technologies such as Ethernet and Token Ring without the limitations of wires or cables. But to view a WLAN just in terms of the cables it does not have is to miss the point: WLANs redefine the way we view LANs. Connectivity no longer implies attachment. Local areas are measured not in feet or meters, but miles or kilometers. An infrastructure need not be buried in the ground or hidden behind the walls—an "infrastructure" can move and change at the speed of the organization. The rapid and wide-spread fascination for new wireless technologies has raised a raging debate over security concerns among scientists, IT professionals and journalists. Scientists come perpetually up with new research results emphasizing the insecurity of the technologies and methods on which WLANs rely. At the same time, we can read from newspapers about corporate suffering from massive damages because of negligent exploitation of WLANs.

Amit Mishra, lecturer , Department of Mathematics/Computer Science, IBB University, Lapai, Nigeria
Dangana Muhammad, Department of Information and Communication Technology at Ibrahim Badamasi Babangida University, Lapai, Nigeria
Joseph Elijah, lecturer ,Department of Mathematics/Computer Science, IBB University, Lapai, Nigeria.
Dinesh Kumar, lecturer in Kebbi State University of Science and Technology, Nigeria

I. Understanding Wireless LAN Classifications and 802.11 Architecture

A WLAN environment has wireless client stations that use radio modems to communicate to an AP. The client stations are generally equipped with a wireless network interface card (NIC) that consists of the radio transceiver and the logic to interact with the client machine and software. An AP comprises essentially a radio transceiver on one side and a bridge to the wired backbone on the other. Hence, the standard defines following two basic network topologies.

A. ***ad hoc wirelessLANs:*** In *ad hoc* mode, each client communicates directly with the other clients within the network, figure 1. *ad-hoc* mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate. If a client in an *ad-hoc* network wishes to communicate outside of the cell, a member of the cell *MUST* operate as a gateway and perform routing.

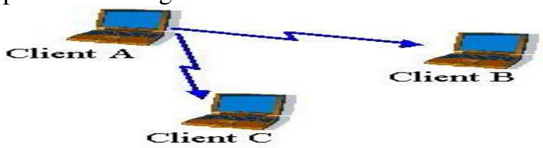


Figure 1: Ad hoc wireless LAN.

B. ***Wireless LANs with Infrastructure:*** In *infrastructure* mode, each client sends all of it's communications to a central station, or access point (AP). The access point acts as an Ethernet bridge and forwards the communications onto the appropriate network– either the wired network, or the wireless network, see figure 2.

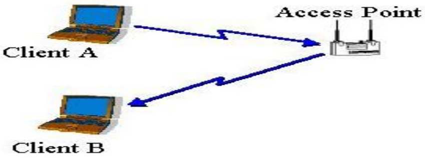


Fig 2: Example infrastructure network

Prior to communicating data, wireless clients and access points must establish a relationship, or an *association*. Only after an *association* is established can the two wireless stations exchange data. In *infrastructure* mode, the clients associate with an access point. The association process is a two-step process involving three states:

a) *Unauthenticated and unassociated*,
b) *Authenticated and unassociated*, and
c) *Authenticated and associated.*

II. Wireless LANs and Its Benefit

Wirelesses LANs are less expensive and less intrusive to implement and maintain, as user needs change.

Simplified Implementation and Maintenance

Wireless APs can be placed anywhere, where they can accommodate a virtually endless variety of office configurations. Wired LANs, in contrast, consume time and resources to run cables from a network closet to user's desktops and to difficult-to-service areas such as conference room tables and common areas. With a wired LAN, each additional user or modification to the floor plan necessitates adjustments to the cabling system.

Extended Reach

Wireless LANs enable employees to access company resources from any location within an AP's transmission range.

Increased Worker Mobility

The roaming benefits of wireless LANs extend across all industries and disciplines. The shop foreman can manage logistics from the warehouse as easily as office-based employees move about the building with their laptops or PDAs. And field sales employees can connect to public wireless LANs in coffee shops and airport lounges.

Reduced Total Cost of Ownership and Operation

The cumulative benefits of simplified implementation and maintenance, an extended LAN reach, and the freedom to roam minimize expenses and improve organizational and employee productivity. The result is reduced total cost of ownership and operation.

III. Security Risks and Technical Challenges of a Wireless Network

Security is a principal consideration when planning, designing, implementing, and managing a network infrastructure. This is especially true for wireless LANs, which present a unique, set of challenges to IT and security professionals. In addition to the typical problems that new network and device technologies endanger, including incompatibilities and ongoing support issues, non-secure wireless LANs can expose an organization's network traffic and resources to unauthorized outsiders.Some of these risks are similar to those of wired networks.Specific threats and vulnerabilitiesto wireless networks and handheld devices include the following:

a) All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.

Malicious entities may gain unauthorized access to an agency's computer network through wireless connections, bypassing any firewall protections.

Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.

DoS attacks may be directed at wireless connections or devices.

Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.

Sensitive data may be corrupted during improper synchronization.

Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements.

Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.

Handheld devices are easily stolen and can reveal sensitive information.

Data may be extracted without detection from improperly configured devices.

Viruses or other malicious code may corrupt data on a wireless device and subsequently be introduced to a wired network connection.

Malicious entities may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities.

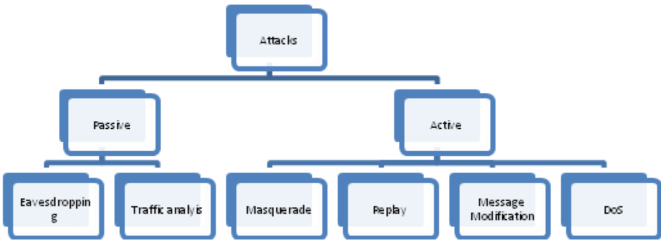
Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

Malicious entities may use third-party, untrusted wireless network services to gain access to an agency's or other organization's network resources.

Internal attacks may be possible via ad hoc transmissions.

IV. Security Threats in Wireless Network

As mentioned above the 802.11 WLAN or WiFiindustry is burgeoning and currently has significant momentum. All indications suggest that in the coming years numerous organizations will deploy 802.11 WLAN technology. Many organizations including retail stores, hospitals, airports, and business enterprises plan to capitalize on the benefits of "going wireless." However, although there has been tremendous growth and success, everything relative to 802.11 WLANs has not been positive.



Network security attacks are typically divided into *passive* and *active* attacks. These two broad classes are then subdivided into other types of attacks. All are defined below.

a) Passive Attack— An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

b) Eavesdropping—The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

c) Traffic analysis—The attacker, in a much subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

b) Active Attack—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.

a. **Masquerading**—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

b. **Replay**—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

c. **Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

d. **Denial-of-service**—The attacker prevents or prohibits the normal use or management of communications facilities.

The risks associated with 802.11 are the result of one or more of these attacks. The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service.

V. Securing a Wireless Network

Security encompasses a number of facets, which is why companies invest heavily in dedicated security infrastructure and highly-trained specialists. Every network application and infrastructure component has a distinct set of security requirements that must be addressed before managers feel comfortable entrusting it with the enterprise's mission critical information. For wireless LAN, security takes place on two levels: the packet level and the radio frequency (RF) level.

a) Data Confidentiality and Integrity

The protection of data as it passes along the shared medium. Confidentiality is delivered through the use of encryption algorithms used to encode information in a manner that can only be decoded and read by the parties for which it is intended. Going hand-in-hand with encryption are the concepts of data integrity and non-repudiation, which help to prevent hackers from altering data. This is achieved through the use of a hashing algorithm which takes a snapshot of each packet's content before it is encrypted.

b) Authentication and Access Control

The mechanisms used to grant authorized users access to the wireless network and the resources residing on the broader enterprise network. A user can potentially have a laptop outside of the office premises, and without an authentication mechanism to keep them out, they could gain full access to the corporate network.

c) Intrusion Detection and Prevention

The aforementioned categories focus on the packet level and borrow heavily from wired network security principles – with unique wireless characteristics. Conversely, intrusion detection and prevention focuses on the radio frequency (RF) level and is entirely unique to WLAN. It involves radio scanning to detect rogue access points or ad hoc networks to regulate network access.

d) Broader Security Considerations

While it is desirable to have the most sophisticated packet-level and RF-level security available, network managers need to make implementation decisions in the context of the following concerns, which are consistent with virtually all network security initiatives:

a. Management will demand that the solution be *cost-effective*, leveraging and integrating with existing security technology where possible, requiring little administrative maintenance and interaction, and representing an overall implementation cost that is commensurate with the initial capital expenditure.

b. End-users will resist any implementation that is not *transparent*. They will expect full access to applications and network resources, and will not tolerate excessive complexity and/or performance degradation resulting from the security infrastructure.

e) Recommendations and Suggestions:

a. Even as new 802.11 vulnerabilities are identified and exploited, organizations can mitigate or eliminate many of wireless LAN's security risks with careful education, planning, implementation, and management. The following steps aid this process:

[1] Wireless LAN Security Policies and Practices must be Established

An effective wireless LAN strategy involves defining, standardizing, documenting, disseminating, and enforcing wireless LAN security policies and practices. These include specifying the make, model, configuration, and settings of the wireless LAN equipment authorized for use, as well as documenting and managing the APs and connected network infrastructure.

[2] Security Design

When placing wireless APs for strategic coverage, installers should consider signal bleed into uncontrolled areas where transmissions can be intercepted. Wireless coverage should be implemented only where needed.

[3] Logically Separate Internal Networks

The LAN segments that connect to wireless APs should connect to a corporate Virtual Private Network (VPN) gateway, but not directly to the production network. Eliminating APs from the production network minimizes the risk of attack techniques such as packet sniffing.

[4] Enable VPN Access Only

Requiring users to connect to the wireless LAN via a VPN is recommended. Once authenticated, authorized users communicate using an encrypted tunnel between the connecting device and the LAN, reducing the risk that a transmission will be captured.

[5] Restricting Unnecessary Protocols

Restricting unnecessary or redundant protocols from the LAN segments that connect the APs to the VPN gateway reduces the possibility of unidentified holes and vulnerabilities. Retaining the Domain Name System (DNS) and IP Security (IPSec) protocols is recommended to support the VPN.

[6] Restrict AP Connections

Administrators can use authorization tables to selectively enable LAN connections only to devices with approved NIC addresses. Each NIC has a unique address that can be added to a table of authorized users; most vendors' APs support Media Access Control (MAC) restrictions through the use of authorization tables. As a result, instead of editing each AP individually, APs can be pointed to a centrally managed database.

VI. Conclusions:

Today, most organizations deploying wireless LANs simply haven't put enough effort into its security – it isn't right, but it is true. Just like in the wired world, organizations only began to take Internet security seriously after there had been a series of highly visible and financially damaging hacker attacks. Only a similar series of public wireless disasters will catalyze the change needed for organizations to take wireless security more seriously.

Wireless networks using the 802.11b protocol are at present inherently insecure and vulnerable to a variety of attacks. Using a laptop with a Wi-Fi card and the right software, an attacker is capable of immense mischief and in theory could be as far as 20 miles away in a safe haven.

Networks which are poorly configured or do not have any encryption being utilized are the most vulnerable.

Many enterprise network managers have resisted the introduction of wireless LAN, delaying the opportunity to reap the numerous benefits to be had in terms of productivity, responsiveness, and TCO reductions. While the absence of an acceptable security standard served as the chief justification for this decision, Siemens HiPath Wireless delivers a secure solution that resolves this problem and makes the enterprise ready for wireless LAN today.

This paper tried to discuss several alternate solutions possible for securing a wireless network requires only careful design, planning and engineering.

References

[1] Park, S.H, Ganz A., Ganz Z. Security protocol for IEEE 802.11 wireless local areanetworks. In Mobile Networks and Applications, Vol. 3, no. 3, p. 237.246. Netherlands, Baltzer ACM Press, 1998.

[2] Levington M. Unlocking the secret of wireless security. In Oen, p. 23 United Kingdom,
Wilmington Business Publishing, Sept. 2002.

[3] Arbaugh, W. A., Shankar, N. and Justin Wan, Y.C. Your 802.11 Wireless Network has
No Clothes, [online], URL: http://www.cs.umd.edu/7Ewaa/wireless.pdf

[4] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer(PHY) specification. IEEE Standard 802.11, 1997 Edition," 1997.

[5] Lucent Orinoco, User's Guide for the ORiNOCO Manager's Suite, Sep 2006.

[6] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," Tech.Rep.03628E, IEEE 802.11committee, March2006.

Dr. Amit Mishra(PhD) is a lecturer in the Department of Mathematics/Computer Science, IBB University, Lapai, Nigeria. His current research interests include: Network security, Cryptology, Machine learning, Software Engineering, Reverse Engineering. He has been publishing in the above mentioned fields in various national and international journals. He is also Microsoft Certified professional in Win2K and Exchange Server.

Mr. Dangana Muhammad received his M.Sc.(Eng.) degree in Communications Engineering from Ahmadu Bello University, Zaria, Nigeria in 2016 He is currently working in the Department of Information and Communication Technology at Ibrahim Badamasi Babangida University, Lapai, Nigeria. His research interests include: Performance modelling and analysis of computer and communication systems, systemic routing schemes in data Communication, Wireless/Mobile systems, Computer Networks and Network Security.

Mr. Joseph Elijah (M.Tech.) is a lecturer in the Department of Mathematics/Computer Science, IBB University, Lapai, Nigeria. His current research interests include: Image processing, Modelling and Simulation, intelligent systems and Computer networks. He is a member of International association of Engineers (IAENG) with membership number.

Mr. Dinesh Kumar (MCA) is a lecturer in Kebbi State University of Science and Technology, Nigeria. His research interests are Artificial Intelligence, Network Security and System Modelling.