JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Wireless Security in Protocol Stack: Wireless Network Security

Ms. Neha Chauhan[1] Dr. Manjot Kaur Bhatia[2], Dr. C Komalavalli[3], Dr. Chetna Laroiya[4]

MCA Student[1], Dr Manjot Kaur Bhatia[2], Dr C Komalavalli[3*], Dr Chetna Laroiya[4]

[1,2,3,4] Department of Information Technology, Jagan Institute of Management Studies, New Delhi

[2]Manjot.bhatia@jimsindia.org,[3] komal@jimsindia.org,[4] chetnalaroiya@jimsindia.org

Abstract: Increasing applications of Wireless Sensor Networks (WSNs) in different application domains have attracted a lot of interest of the research community. Due to deployment of the sensor network in the remote area, the network is vulnerable to a number of security threats and vulnerabilities. It is found that attackers have different mechanisms to bypass the security trap implemented to secure the organization network. The aim of this study was to review some literatures on wireless security related to the threats, vulnerabilities and some solutions at various layers of TCP/IP protocol.

Keywords - Wireless network, network security, WAP2, WEP, hackers, Firewall

1. INTRODUCTION:

Wireless networks are computer networks that are not connected by cables of any kind. It is a network that uses wireless for the communication among nodes and radio frequency signals are used for the purpose. They are also known as Wi –Fi network and widely used by the people in the current scenario. These networks are gaining popularity nowadays because of their convenience, cost, productivity and nature of the setup. They can be easily integrated with the other type of networks. This network is widely adopted in offices, houses and public areas also due to its convenience. These networks are classified as Wireless LAN, Wireless MANs and Wireless WANs with respect to their area coverage.

Wireless Security refers the avoidance of unauthorized access to computers or data using wireless networks that includes WiFi Network also. This is also referred as WiFi protection, targets to avoid unauthorized users get permission of the network. This leads to the adverse effect to the integrity, confidentiality and availability of the network. Compared to wired network, wireless network is more prone to the security attacks because of its architecture.

WiFi protection can be achieved by Wireless Security Protocols consisting of Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WPA is he authentication protocol designed for Wi-Fi protection.

Availability, Authenticity, Integrity, Confidentiality and Nonrepudiation are most important aspects of wireless security. Authenticity ensures the guaranteed communication between the nodes which are available and authenticated. Confidentiality is the primary concern of wireless network since it ensures that only desired user can understand the message, but not by anyone else. Integrity guarantees the message from Node A to Node B without any modifications during the transmission. Non- repudiation ensures the ability to prevent a denial in an electronic message or transaction.

In this paper, we have analysed the various security challenges of wireless network and solutions to that.

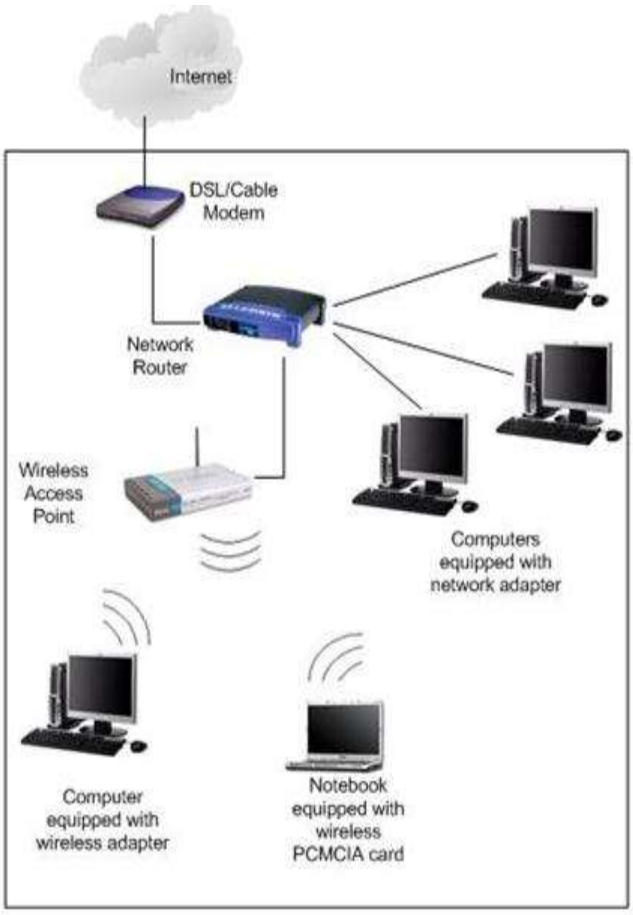

Figure 1: Showing the architecture of wired network and wireless network (for devices accessing Wireless Access

2. LITERATURE REVIEW

Author[1] described about various network threats in the wireless environment and suggested the parameters for achieving secured network.

Authors[2] explained about the routing protocols and attacks on routing protocols in detail. Many networks can be viewed as mutihop network. They discussed the various security issues of routing protocol also.

Authors[3] reviewed the literatures in the area of attacks, threats and vulnerabilities. Attackers have different ways of bypassing the security developed by organizations. Only one weak point paves the way for the attack of whole network of an organization. They suggested that with the help of firewall in every access point can protect the data of the whole organization.

Since Denial of Service compromises the availability and integrity of broadband wireless network, DOS is the most important security threat as per author's view[4] in their publication.

Routing and Security Issues[5] of mobile Adhoc network attracted the attention of the researchers.[5[, In order to provide secure communication, we have to understand the nature of attack. They can be active and passive attacks and attacker can in insider or outsider. Insider is an authorized user of the network and become integral part of the routing mechanisms.

P. Guo et . al[6] derived the applicability, limitations and security architectures of existing Internet Protocols in the context of Internet of Things. They suggested the IP-based security solutions and emphasised specific technical limitations of standard IP security protocols.

Researchers [7] suggested that understanding of security attacks is the way to defend the security issues of wireless network. They described the overview of the wireless network, drawbacks of wireless network, security and privacy issues. Unauthorized access, Active eavesdropping and denial of service are the most potential threats in the network. They recommended the various techniques such as Wireless Network Auditing , change SSID etc.. for the secure communication in the wireless network.

In this paper[8], security attacks and threats in the current scenario such as wireless secret data, MAC address spoofing, DOS etc.. are discussed in detail. Authors adopted a qualitative approach to investigate issues related to wireless networks as well as protocols and solutions against attacks. The risks associated cannot be removed but it is possible to attain a realistic level of security with the help of procedures and approaches to assess, evaluate, manage and prevent risks.

3. SECURITY ATTACKS IN WIRELESS ENVIRONMENTS

Among the threats, some can rise up in any networking environment (i.e. denial of service) even as others are particular to wireless (i.e. rogue get right of entry to and passive taking photographs). Let's test some:

a) DENIAL OF SERVICE

Denial of service is a clean attack this is predicated on restricting get right of entry to services on a harassed network. This hack is applied by routing a great amount of web page traffic to a machine with specific purpose. With this technique, the immoderate amount of web page traffic overwhelms the purpose machine and disrupts service. It is also feasible for hackers to launch a denial of service attack by disrupting the signal on the network. This can be accomplished by creating enough interference on one channel to interrupt the service.

b) ROGUE ACCESS POINT

A rogue access point is a wireless access point is similar to the access point. It is installed on a secure network without explicit authorization from the administrator of the local network administrator. Rouge point is not monitored by the system administrator and act as a security breach.

c) PASSIVE CAPTURING

Passive capturing or monitoring is a an attacking technique. This is used to capture traffic from a network by copying complete traffic. This traffic is copied often from the spam or mirror port, Also network trap could capture the traffic.

d) IDENTITY THEFT (MAC spoofing)

The Sybil attack is where a node misleads other nodes by showing ID other than its own ID. T shows the ID of the other many nodes who are authentic nodes of a network[9].

e) NETWORK INJECTION

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree". The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

f) CAFFE LATTE ATTACK

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in minutes.

S.No.	Attack	Layer
1.	Denial of Service	Application
2.	Rouge attack	MAC
3.	Passive Capturing	Network
4.	Sybil	Network [10]
5.	Network Injection	MAC, Network
6.	Caffe Latte	Application

Figure 2: Attacks on various layers of TCP/IP

4. SOLUTIONS TO WIRELESS SECURITY THREATS

4.1Cryptography

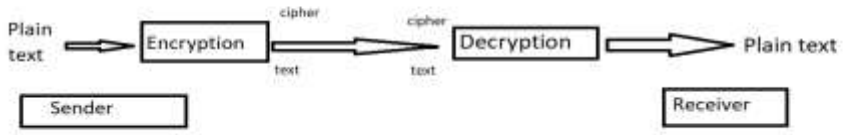

Figure 2: Working of cryptography

Cryptography is a technique by which you can convert plaintext into ciphertext. and convert ciphertext back to plaintext. Plain text is a message that anyone can read and understand, but ciphertext is a message that can also be called a secret message, anyone can read it but cannot understand. Cryptography is used for confidentiality. Confidentiality means no one can take my message. For example, I send a message to a person 1000 km away, in the meantime an unauthorized user can trace that message to that packet but it does not mean that he can read that message and understand it,so that is what the meaning of confidentiality. To send a message from sender to receiver, we use the Internet, there is not any secure link, then an unauthorized user can trace that message in the middle, but if it is in the message plaintext, then any user can understand ,To solve that problem we use cryptography.

So what we do in cryptography is that send a message uses encryption algorithms. What do those algorithms do, they use a key, to convert the text into ciphertext. Then as that message goes to the receiver, the receiver decrypts that message. So we get the confidentiality from encryption and we will call this whole method Cryptography.

Cryptography uses these two methods symmetric-key and Asymmetric-key. Symmetric-key means that the same key with which it is encrypted will also be decrypted. Asymmetric means encrypt with one key and can decrypt with another key.

Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on. Today's enterprise weather is predicated upon collecting, studying and (extra importantly) sharing critical facts approximately your enterprise and its customers. Data encryption may be used to stable the Wi-Fi networks, Using Virtual Private Networks and Secure Socket Layers this information is shared.

Talking about types of encryption, there are Symmetric Encryption, Asymmetric Encryption and Hybrid Encryption. In symmetric encryption, data is encrypted and decrypted using a single key and symmetric encryption is the primary use for data encryption.

We use three types of algorithms in symmetric encryption, first DES symmetric encryption algorithm, second 3DES symmetric encryption algorithm and third AES symmetric encryption algorithm. These algorithms also have many advantages. Key pair is used in asymmetric encryption for encryption-decryption and can also be called primary key and public key. In asymmetric encryption we use algorithms such as RSA, ECC etc. Hybrid encryption is symmetric encryption plus asymmetric encryption.

4.2 Firewalls

With the implementation of firewall the organisation can set up a sturdy protection for the data. Data packets coming from the external environment to the organization are filtered by the firewall. There are many predefined parameters of the fire wall which a data packet has to comply with. Firewall blocks the packet at the gateway itself. Firewall can be hardware or software or it can also be a combination of both.

4.3 Intrusion detection

Intrusion detection and prevention software program, additionally discovered in stressed and Wi-Fi networks, offers your community with the software program intelligence without delay discover and halt and assaults, threats, worms, viruses and extra.

4.3 Use anti-virus and anti-spyware software, and a firewall

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

4.4 Turn off your wireless network

Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

4.5 Authentication

Authentication and identity techniques defend the stable information for your community. In addition to password safety, answers consisting of key fobs and biometric authentication make certain that most effective people with right authority to get admission to your stable information can do so, making your Wi-Fi community secure.

How can we verify any user, it is called authentication. There are two types of users, sender and receivers, so those who pass the information is sender. Both should be authenticated.

There are three types of Authentication- Message Authentication, Message Authentication code (MAC) and third is Hash function.

Message Authentication-we use cypher text authentication in message authentication.

Message Authentication code (MAC)- C(M,K)=Fixed size code

Hash function -H(M)=Fixed size code(Hash code)

4.6 Allow only specific computers to access your wireless network

Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

4.7 Use anti-virus and anti-spyware software, and a firewall

Any Computer on a wireless network needs the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

4.8 Don't assume that public "hot spots" are secure

Many hospitals, hotels and railway stations and other public establishments provide wireless networks to their customers.

Security Solution	Countermeasure against Attack
Firewall	Against hardware level attack
Cryptography	Against Information breach
Intrusion Detection	Against the application layer attacks
Turning off the WSN	To safe guard against the Data Link attack
Authentication	Sybil attack
Allowing only specific computers to access the WSN	Hardware level attack
Hot spots	Application level attack

Figure 3: Security solution under different categories

5. CONCLUSION

This paper gives the concept of wireless sensor network. In any unattended area the WSN is much prone to security attacks. This paper summarizes various security attacks and also categorizes its countermeasure under different category. This paper lists various security schemes for wireless network. In future this work could be extended to map the possible security attack with the specific layer in protocol stack.

References

1) Shailja Pandey, "Modern Network Security: Issues and Challenges" in an International Journal of Engineering Science and Technology, Vol. 3 No. 5 May 2011
2) Yang Xiao, Hui Chen, Shuhui Yang, Yi-Bing Lin, and Ding-Zhu Du in an EURASIP Journal on Wireless Communications and Networking Volume 2009, , 3 pages
3) Lusekelo Kibona, Hassana Ganame," Wireless Network Security: Challenges, Threats and Solutions. A Critical Review", in an International Journal of Academic Multidisciplinary Research (IJAMR) ISSN: 2000-006X Vol. 2 Issue 4, April – 2018, Pages: 19-27
4) S. Khan, K.-K. Loo, T. Naeem, and M. A. Khan, "Denial of service attacks and challenges in broadband wireless networks," 8; 7, 2008.
5) P. Kumar, "Analysis of different security attacks in MANETs on protocol stack A-review," in In International Journal of Engineering and Technology (IJEAT), ISSN: 2249-8958, Volume-1, Issue-5, 2012, 2012.
6) P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication Wireless Personal Communications, vol. 61, pp. 527-542, 2011.
7) Muhammad Imran Tariq, "WIRELESS SECURITY AND THREATS", Proc. ICCS-11, Lahore, Pakistan December 19-22, 2011, Vol. 21, pp. 717-729
8) Somya Khidir Mohmmed Ataelmanan, Mostafa Ahmed Hassan Al," A review of threats, protocols, and solutions to enhance the security of wireless networks", IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.4, April 2019
9) Mohamed-Lamine Messai, "Classification of Attacks in Wireless Sensor Networks" April, 2014
10) Jaydip Sen, "Security in Wireless Sensor Networks"