RESEARCH ARTICLE OPEN ACCESS

Sensor Networks for Emergency Response: Challenges and Opportunities

R.Karthikeyan[1], Shanmugapriya M[2] , Indhu P[3]

[1] Asst.Prof, Dept of MCA, Gnanamani college of Technology, Namakkal, INDIA.

[2,3] P.G.Scholar, Dept of MCA, Gnanamani college of Technology, Namakkal, INDIA.

--************************----------------------------------

Abstract:

Wireless networking is inherently insecure. From jamming to eavesdropping, from man-in the middle to spoofing, there are a variety of attack methods that can be used against the users of wireless networks. Modern wireless data networks use a variety of cryptographic techniques such as encryption and authentication to provide barriers to such infiltrations. An overview of the advantages that wireless networks have over wired technology is then given. The paper also advances some of the major security risks that wireless networks face. It is at such security holes that the information criminals tend to attack. In this paper, we identify the various security related challenges faced by wireless protocols. This study is useful as it provides lessons for ICT managers, directors, academia and organizations, who wish to develop install or are already using wireless networks within their offices.

Keywords —**Blue Tooth, WEP**

--************************--

1. Introduction

The invention of the computer and the subsequent creation of communication networks can be hailed at the most significant accomplishment of the 21st century. This invention has transformed the way in which communication and information processing takes place. The backbone of the vast communication network is made up of fixed connections which mostly utilize fiber optics as well as.

2. Wireless networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD) and Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are “tether less”—they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band.

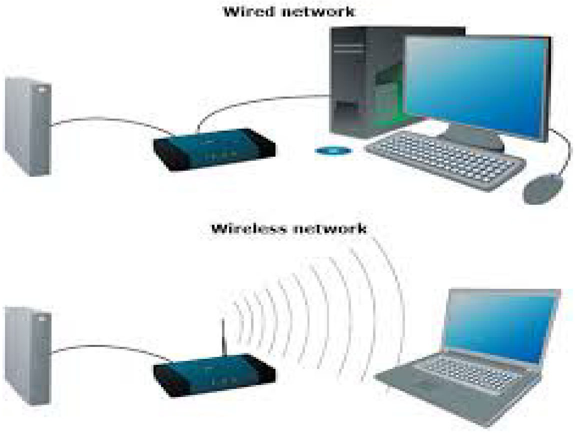
3. Wireless Technologies

There are a myriad of wireless technologies and they differ in the amount of bandwidth they provide as well as the distance over which the nodes in the network can communicate. There are four prominent wireless technologies which are; Bluetooth, WiFi, WiMAX and 3G cellular wirelesses.

A. Bluetooth

Bluetooth (IEEE 802.15.1) is the technology that is employed to undertake short-range communication between notebook computers, PDAs, mobile phones and other personal computing devices. The technology is more convenient than connecting devices with a wire to communicate. Bluetooth operates in a license free band at 2.45GHz and the communication range is about 10m and due to this short range, the technology is sometimes categorized as a personal area network

B. Wired Equivalent Protocol (WEP)



This article, from an academic, peer-reviewed journal specializing in wireless communications, details recent findings on how a practical key recovery attack on Wired Equivalent Protocol (WEP), based on partial key exposure vulnerability in the encryption being used (RC4 stream cipher) can be used as a flaw in breaking WEP. The article describes how to apply the flaw in breaking WEP and concludes that the protocol also referred to as 802.11b WEP standard by the Institute of Electrical and Electronic Engineers Inc, is not secure. It details recent findings on how the Wired Equivalent Privacy (WEP) protocol lacks the ability to exchange its encryption keys safely key and has from severe cryptographic issues to the extent that secret service personnel have used public lectures to demonstrate how easy it is to break into a 128-bit WEP key in less than five minutes.

4. Wired and Wireless Networks

This article, originates from, an ACM International Conference whose researchers are based at the Los Angeles University in the Computer Science department Engineering department. The article suggests that connections using the 802.11 protocol in wireless Local Area Network (LANs) are reasonably good and as such that is what makes them widely used in educational institutions and scientific research laboratories. Information from this article will help us produce a more credible research proposal as it objects to the common notion that the WEP protocol is not suitable for wireless technology.

- ❖ **Privacy:-**

This article, from an academic, peer-reviewed journal specializing in wireless location privacy, details recent findings on how a practical key recovery attack on Wired Equivalent Protocol (WEP), based on unauthorised person could track a user's position. In addition, they suggest that interface identifiers which uniquely identify each client, allows tracking of locations over time. The study supports what was said earlier by Mahajan, R (2006) and also suggests that using MAC is not sufficient and that mechanisms should be rebuilt for privacy.

- ❖ **Security:-**

This article is an academic journal and originates from, the Columbus State University It also discusses the evolution of the WLANs and suggests that the early versions of wireless networks weren't meant to be consumed the way it did. The information in this article will help support our research proposal which suggests that WLANs data transmitted by radio waves exposes the organisation to security risks such that the integrity of confidential data held on any of their networks using the known standards such as 802.11 protocols is not reliable

5. WPA and WPA2 Protocols

This article, from an academic, journal specializing in the WPA and WPA2 Protocol, details recent findings on why the WPA protocol was developed and what vulnerabilities it was created for. The article further describes that the WPA adopted the key management system or Temporary Key Integrity Protocol (TKIP). The article however suggests that the protocol uses keys generated by the server, which even though dynamically created still leave room for the keys to be hacked into. This study acknowledges the use of Message Integrity Checks

(MIC) in order to militate against the keys being cracked.

6. MODEL ANALYSIS

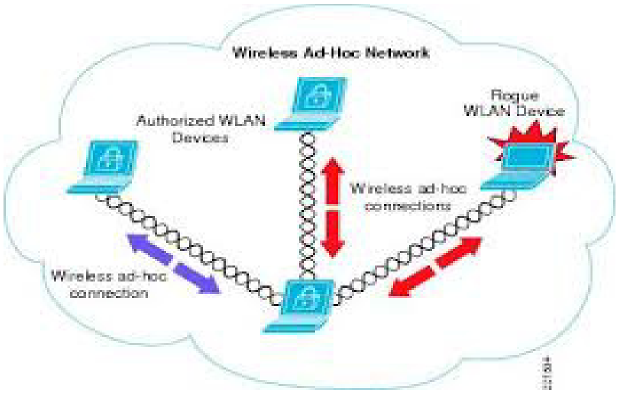
Modern wireless networks represent new technology which unfortunately retains sufficient deficiencies for enemies to commit old style crimes upon them. In search of adequate security the Institute of Electrical and Electronic Engineers (IEEE) has sought to establish protocols that can guarantee the secure connections to wireless networks . With this the IEEE has had some success but has not taken on a by product of using wireless networks into consideration; radio wave leakage. Various researchers have proposed novel projects to be used in securing wireless access points and suggested that they were developed for the next generation. This will be of great benefit to this study as the paper can draw on the experiences of the researchers in developing and simulating a wireless test bed It has been suggested that the different techniques used to protect wireless networks, stem from the standards and protocols released by the IEEE, which should be updated as and when they are release. The study found that the flaws which are to be updated usually stem from encryption, equipment security settings and rogue access points. "A firm can build more effective security strategies by identifying and ranking the severity of potential threats to it's information systems efforts" (Whitman 2003). This study by a Security researcher warned of the inherent dangers facing financial organisations and what the cost to the financial industry was going to be.

- **WIRELESS PERSONAL AREA NETWORK (WPAN)** – a small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables. Examples include print services or enabling a wireless keyboard or mouse to communicate with a computer.
- **WIRELESS LOCAL AREA NETWORKS (WLANS)** are groups of wireless networking nodes within a limited geographic area, such as an office building or campus that are capable of radio communications. WLANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility.

- **WIRELESS METROPOLITAN AREA NETWORKS (WMANS)** can provide connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas.

- **WIRELESS WIDE AREA NETWORKS (WWANS)** connect individuals and devices over large geographic areas. WWANs are typically used for mobile voice and data communications, as well as satellite communications.

7. AD HOC NETWORKS



Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed "ad hoc" because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a master-slave system connected by wireless links to enable devices to communicate. In a Bluetooth network, the master of the piconet controls the changing network topologies of these networks.

8. LAYERED SECURITY FOR WIRELESS NETWORKS:

A layered approach to wireless security can provide a high degree of protection and leverage existing network security investments. The layered approach consists of the following four levels:

- **Wireless deployment and policy**
- **Wireless access control**
- **Perimeter security**
- **Application security**

When implemented, as discussed below, the layered approach can make a WLAN more secure than a typical wired network by centralizing points of access, implementing manageable device-level security and governing internal access with firewall-level policies. Security professionals speak in terms of work factor, which is an important concept when implementing layered security.

LEVEL1-WIRELESS DEPLOYMENT AND POLICY

Best practices for wireless deployment and policy are: Deploy the minimum number of WAPs needed for adequate Coverage. Set WAP broadcast power to the lowest practical level.

- **Installation of WAPs**
- **NIC operational mode**
- **WLAN user-group access,**
- **including employees,**
- **visitors**
- **Contractors**

The physical deployment of wireless networking devices is the foundation on which a secure environment is created. The basic rule of thumb maintains that one does not over design the wireless network. The goal is to avoid broadcasting where it is not necessary. For example, four WAPs should not be installed in a space where one would suffice or in areas that do not need access to the network, such as the building entrance waiting room. More is not necessarily better.

LEVEL2—WIRELESSACCESS CONTROL

Best practices for wireless access control include:

1. Configure the WEP for the highest level of encryption.
2. Change the SSID regularly, where practical.
3. Do not broadcast the SSID.
4. Verify the media access control (MAC) address upon device connection.
5. Maintain and enforce access policies for unauthorized/unrecognized devices.

LEVEL 3-PERIMETER SECURITY

Best practices for perimeter security include:

1. Install an intrusion prevention system and wireless firewall on WLAN.
2. Encrypt WLAN traffic using a virtual private network (VPN).
3. Direct all traffic through the VPN server and configure clients appropriately.
4. Maintain and enforce VPN routing and access policies.

VPN technology provides a method for securing traffic that moves across entrusted network segments, such as the Internet or the WLAN. A VPN is essentially an extension of a private network that encompasses encapsulated, encrypted and authenticated connections. VPN encryption algorithms are Complex and extremely difficult to compromise. VPN connections should be required for all WLAN traffic.

LEVEL-4-APPLICATION SECURITY

Best practices for application security include:

- ✓ Implement an application-level user authentication system.
- ✓ Maintain and enforce permissions and password policies.
- ✓ Install vendor patches as they become available.

CONCLUSION

This paper set out to discus wireless networks which are increasingly becoming preferred over wired networks by many users. The paper began by offering an overview of networking and then proceeded to define wireless networking and discuss the various technologies that are used.

REFERENCES

1. 1. GH. Muhanna Computer Wireless Networking and Communication International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013 ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021 .
2. R.Karthikeyan," Improved Apriori Algorithm for Mining Rules" in the International Journal of Advanced Research in biology Engineering science and Technology Volume 11, Issue 4, April 2016, Page No:71-77.
3. R.Karthikeyan, & et all "Honeypots for Network Security", International journal for Research & Development in Technology.Volume 7.Issue 2 ,Jan 2017,Page No.:62-66 ISSN:2349-3585.
4. R.Karthikeyan,"A Survey on Position Based Routing in Mobile Adhoc Networks" in the international journal of P2P Network Trends and Technology, Volume 3 Issue 7 2013, ISSN:2249-2615, Page No.:81-88.
5. 2. S. Gopalakrishnan A survey of wireless network security,International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X IJCSMC, Vol. 3, Issue. 1, January 2014, pg.53 – 68.
6. R.Karthikeyan,"A Survey on Sensor Networks" in the International Journal for Research & Development in Technology Volume 7, Issue 1, Jan 2017, Page No:71-77.
7. R.Karthikeyan, & et all "Web Based Honeypots Network",in the International journal for Research & Development in Technology.Volume 7.Issue 2 ,Jan 2017,Page No.:67-73 ISSN:2349-3585.
8. R.Karthikeyan, & et all,"A Simple Transmit Diversity Technique for Wireless Communication",in the International journal for Engineering and Techniques. Volume 3. Issue 1, Feb 2017, Page No.:56-61 ISSN:2395-1303.
9. R.Karthikeyan, & et all "Strategy of Trible – E on Solving Trojan Defense in Cyber Crime Cases", International journal for Research & Development in Technology.Volume 7.Issue 1 ,Jan 2017,Page No.:167-171.
10. C. Ijeh1, Allan J. Brimicombe, David S. Preston Chris .O. Imafidon Security Measures in Wired and Wireless Networks Anthony , pg 113-12.
11. Karthikeyan, & et all"Advanced Honey Pot Architecture for Network Threats Quantification" in the international journal of Engineering and Techniques, Volume 3 Issue 2, March 2017, ISSN:2395-1303, PP No.:92-96.
12. R.Karthikeyan, & et all "Estimating Driving Behavior by a smart phone" in the international journal of Engineering and Techniques, Volume 3 Issue 2, March 2017, ISSN:2395-1303,PP No.:84-91.
13. R.Karthikeyan, & et all "SAMI: Service-Based Arbitrated Multi-Tier Infrastructure for Cloud Computing" in the international journal for Research & Development in Technology, Volume 7 Issue 2, Jan 2017,ISSN(0):2349-3585, Pg.no:98-102
14. R.Karthikeyan, & et all "FLIP-OFDM for Optical Wireless Communications" in the international journal of Engineering and Techniques, Volume 3 Issue 1, Jan - Feb 2017, ISSN:2395-1303,PP No.:115-120.
15. R.Karthikeyan, & et all "Application Optimization in Mobile Cloud Computing" in the international journal of Engineering and Techniques, Volume 3 Issue 1, Jan - Feb 2017, ISSN:2395-1303,PP No.:121-125.
16. R.Karthikeyan, & et all "The Sybil Attack" in the international journal of Engineering

and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:121-125.

17. R.Karthikeyan, & et all ”Securing WMN Using Hybrid Honeypot System” in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:121-125.

18. R.Karthikeyan, & et all ”Automated Predictive big data analytics using Ontology based Semantics” in the international journal of Engineering and Techniques, Volume 3 Issue 3, May – Jun 2017, ISSN:2395-1303,PP No.:77-81.

19. R.Karthikeyan, & et all ”A Survey of logical Models for OLAP databases” in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:171-181.

20. R.Karthikeyan, & et all ”A Client Solution for Mitigating Cross Site Scripting Attacks” in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13063-13067.

21. 4.Jordan, R & Abdallah, C 2002, “Wireless communications and networking: an overview”, IEEE Antenna's and Propagation Magazine, 44 (1): 185-193.

22. R.Karthikeyan, & et all ”A Condensation Based Approach to Privacy Preserving Data Mining” in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13185-13189.

23. R.Karthikeyan, & et all ”Biometric for Mobile Security” in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13552-13555.

24. R.Karthikeyan, & et all ”Data Mining on Parallel Database Systems” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:13922-13927.

25. R.Karthikeyan, & et all ”Ant Colony System for Graph Coloring Problem” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14120-14125.

26. R.Karthikeyan, & et all ”Classification of Peer –To- Peer Architectures and Applications” in the international journal of Engineering Science & Computing, Volume7,Issue8, Aug 2017, ISSN(0):2361-3361,PP No.:14394-14397.

27. R.Karthikeyan, & et all ”Mobile Banking Services” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14357-14361.

28. Simmons G. J, “The Prisoners Problem and the Subliminal Channel”, Proceedings of crypto ’83, Plenum Press, pp 51-67, 1983.

29. R.Karthikeyan, & et all ”Neural Networks for Shortest Path Computation and Routing in Computer Networks” in the international journal of Engineering and Techniques, Volume 3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:86-91.

30. R.Karthikeyan, & et all ”An Sight into Virtual Techniques Private Networks & IP Tunneling” in the international journal of Engineering and Techniques, Volume 3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:129-133.

31. R.Karthikeyan, & et all “Routing Approaches in Mobile Ad-hoc Networks” in the International Journal of Research in Engineering Technology, Volume 2 Issue 5, Aug 2017, ISSN:2455-1341, Pg No.:1-7.

32. Anderson R. J, “Stretching the Limit of Steganography”, In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48, 1996.

33. R.Karthikeyan, & et all “Public Key Infrastructure Using Wireles Commnication Networks” in the International Journal of Computer Techniques, Volume 4 Issue 4,

Aug 2017, ISSN:2394-2231, Pg No.:154-158.

34. Mitchell Ashley , "A Guide to Wireless Network Security" Information systems Control Journal ,Volume 3,2004.