IJERST International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 3, No. 3, August 2014
© 2014 IJERST. All Rights Reserved

Research Paper

THE ENHANCEMENT OF WIRELESS FIDELITY (WI-FI) TECHNOLOGY, ITS SECURITY AND PROTECTION ISSUES

A Rajalakshmi[1]* and G Kapilya[2]

Corresponding Author:* ***A Rajalakshmi* ✉ *rajalakshmi060595@gmail.com*

Nowadays communications through mobiles, computers, laptops, wireless networking technologies have extended to a great level. This does a maximum coverage all over the world. Security issues has also been crossed a level in Wi-Fi network because of the unauthorized users and the Wi-Fi hackers. So to implement the possible Security WEP, WPA, as has been proposed in this paper to overcome the possible security problems. These both protocols are generally used to encrypt the current data and information, so that the unauthorized and hackers cannot be able decrypt the data and hack the Wireless Fidelity (Wi-Fi) networks. Many accessories can be linked with the Wireless Fidelity network with the help the Access Point (AP). Universal Mobile Telecommunications System (UMTS) network is also compared with Wi-Fi Network for better performance in the security and also for the authorization purpose.

Keywords: Wireless Fidelity Technology, Wired Equivalent Privacy (WEP), Wireless Fidelity Protected Access (WPA), Wireless Access Point

INTRODUCTION

Wireless Fidelity Wi-Fi Technology is one of the upcoming technique in the internet world. This Wi-Fi can be a substitute to Wired Technology. Wi-Fi is generally used for linking devices in wireless form. Wi-Fi Network attach computers to one another in a better communicable way. It create a invisible path between the internet and the wired network. Wi-Fi network working can be done on the physical and the data link layer. Radio Frequency (RF) is used for transmitting data through air. This is the very feature in the Wi-Fi technology. It also provides better data speeds. IEEE 802.11 is considered as a position of values moving elsewhere can be known as Wireless Local Area Network (WLAN). This is also a type of network communication.

Access Point (AP) is considered as very important feature in the Wi-Fi network technology. Access Point (AP) have a radio transmitter and also a radio receiver. This directly gets connected with the wired network or to the internet network. This Access Point (AP) take a common achievement as a base station for the entire Wi-Fi net-

[1] Department of Information Technology, Saveetha School of Engineering, Saveetha University, Thandalam, Chennai, Tamil Nadu.

[2] Department of Computer Science, Saveetha School of Engineering, Saveetha University, Thandalam, Chennai, Tamil Nadu.

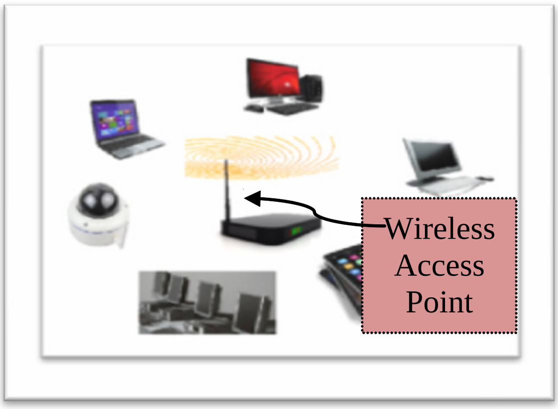
Figure 1: Wireless Fidelity Technology

work. Some of the Wi-Fi Network Topologies are given below.

- Access Point AP-based topology
- Star-based network topology
- Peer-to-peer topology
- Point-to-multipoint bridge topology

This Wi-Fi network is facing many security problems because of the hackers and also by the unauthorized members. The Wi-Fi hacker uses the Wireless Hacking tools AirSnort, Aircrack, WepAttack, WEPCrack etc above the network.

Figure 2: Wireless Access Point



Wireless Access Point is shown in the Figure 2. It basically helps to connect with devices likes digital cameras, tablet computers and digital audio players, PCs, video-game comforts, smart phones, laptops etc.

RELATED WORK

The Wi-Fi signals provide an effect called interference. It has been considered on the channels known as ZigBee channels. In this paper, Packet Error Rate has been linked with the Wi-Fi Signals. Then the Packet Error Rate (PER) is connected with ZigBee channels and the calculations are done. Here Packet Error Rate gets raised when the Wi-Fi Channel comes closer. Band-Limited AWGN concept is also used perfectly in ZigBee channels. Indoor piercing surroundings can also be taken for the testing purpose. Tulin Mangir *et al*., 2011).

Fingerprinting and Triangulation positions can be used here. Fingerprinting can be considered as a real-time process for positioning method. Wireless signals provides superior and the advanced usage more than the Global Positioning System (GPS) signals. Wireless signals charges high exactness. Wi-Fi can be used in the outside and also in the surroundings. In the further process, WLAN network can be compared with the Wi-Fi Signal. Speech recognition, Mobile GIS can be used for Wi-Fi based navigations. All the proposed methods are really effective and successful (Jiangfan Feng and Yanhong Liu, 2012).

In this paper, we have used dynamic neural networks which can be used to provide one of the most excellent evaluations for authenticable research. Optimization technique can be processed typically in the surroundings. LAD technology is implemented and this Localization

Algorithm with Dynamic neural network i.e. LAD have the capacity to decide the RSS variation crisis. Mainly this paper shows the collision of motionless process. This process can be done in the some residence and observed clearly. The outcome which is simulated is an extra more pragmatic and most reasonable (Djabri Fahed and Rongke Liu, 2013).

Wireless health proficiency can be initialized as a special technique. Further wireless message technique was introduced, then the doctors started using it for the heart malfunction patients for guiding and monitoring them in a better way. This monitoring skill in the patient's heart can come across the disease and sickness present inside their body. The feedback can be given in the form of providing necessary treatment for the particular disease. This technique is generally used for the people who are suffering from the death and this provides a better solution to minimize the ratio of death (R S Deshmukh, 2013).

In this paper we have taken effort to inspect rats with the help of radiofrequency radiation. The main thing used here is indoor Wi-Fi network contact plans. Even the Standard wireless gateways can be used in the process for communication purpose. The outcome of this paper is that the DNA damages because of coverage problem. In this case, the catalase and glutathione peroxidase levels getting reduced which are commonly very energetic. Radio Frequency (RF) designs can be used in the transmission of signals and also provides efficient outcome. Security can be provided for the public with the help of the Wi-Fi network contact plans (Atasoy HI, 2012).

Normally Wi-Fi position fingerprinting have to support the interior positioning and this have an effect on the positioning precision. When this process is done, we can analyze and observe the benefits. RSS analyses that accuracy can be improved in better sense. Access Point have the capacity to decrease rapidly as soon as possible. The act of the handheld devices is given through fewer sensitive Wi-Fi chipsets in fact it desire extremely comparable with the act of the PC note pad with additional responsive chipset. The accessibility present in the direction will be in sequence might not be amplifying the positioning accuracy (Gints Jekabsons, Vadim Kairish *et al*., 2011)

Wi-Fi products have a better scope in the Internet world. Wi-Fi network hold up roaming with various devices like cell phones, PC and also with portables accessories like laptops. Through Wi-Fi gaming is also possible. Wired Equivalent Privacy are used for the security reason and also it develops better verification, permission, encryption potentials gradually. Wi-Fi Protected Access can be formed with the assistance of the Wireless Fidelity Alliance. Here Wireless Access Points (APs) provides very secured data for the transmission purpose. Commercial Wi-Fi can be used in enlarge places like college, companies, airports etc. Some kind of operation problems occurs when the connectivity speed is slow (Vandana Wekhande, 2006).

In this paper, Automatic Meter Reading i.e. AMR is used for receiving information and data and then sending the received data to the appropriate network. Energy Saving-Based Hybrid Wireless Mesh Protocol is latest thing proposed in this paper. This kind of algorithm will be appropriate for the Wi-Fi based networks. Hybrid Wireless Mesh Protocol (HWMP) develop the power in a enhanced approach. It display a outcome in which the life cycle of network is extremely enlarged. Energy Saving-Based Hybrid Wireless Mesh Protocol have a better scope in this process (Li Li *et al*., 2013).

SNR-based admission managing scheme is used to tackle the network problem. Wi-Fi based vehicular systems are uses this scheme. It will strictly improve the network ability and the whole scalable capacity. For the better security purpose we can provide mediators like anti-virus, personal firewall etc. Network admission control technology usually uses rebellious equipments to deprive the contact with the particular network. Verification, permission and communication must be done by the respected networks (Kihun Kim *et al*., 2011).

PROBLEM STATEMENT

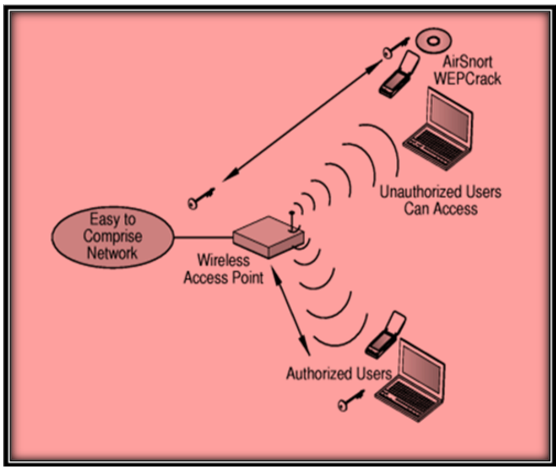
Some kind of unofficial contact will completely harm the computers, mobile phones, etc using the wireless networks. Even the Wi-Fi can be hacked by the hackers. So security is lacking in the Wireless Fidelity technology. To overcome this type of problem some methods has been proposed as follows.

PROPOSED WORK

People feel very easy to use the internet facility from the Wireless Access Point. For this type of security problem, in this paper I have proposed two strong securities. One is known as Wireless Fidelity Protected Access (WPA). The second one is referred as Wired Equivalent Privacy (WEP). To look after the data from interfering eyes we have to go with a concept called encrypting the present data. Nowadays majority of the wireless equipments comes equally Wired Equivalent Privacy and Wireless Fidelity Protected Access.

Wired Equivalent Privacy (WEP) most important weak point is that, it makes use of static or fixed encryption keys. Consider if you connect a Wi-Fi Router along with a Wired Equivalent Privacy (WEP) encryption key, and this must be utilized with each and every device. Then your system or the particular network will encrypt the packets which all it receiving, it will be further transmitted. This WEP is strictly considered to produce a natural security and protection in the wireless communication technique.

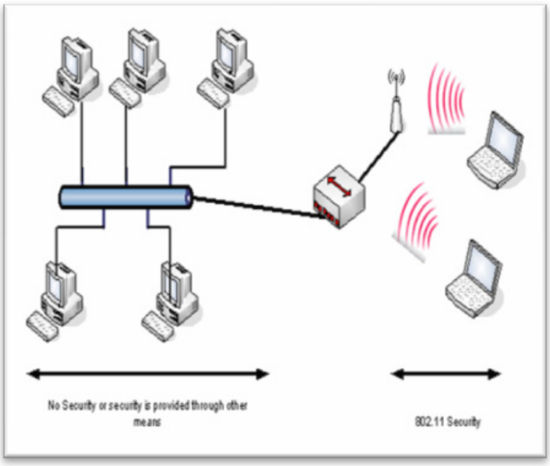
Figure 3: WEP Standard



In the Figure 3, Wired Equivalent Privacy (WEP) for securing wireless networks is shown. In this figure the wireless Access Point (AP) is used by both the authorized users i.e. verified users and also by the unauthorized clients. Some kind of sensible WEP cracking can be simply verified with some equipments such as Air crack etc. AirSnort have the excellent capacity to crack the Wired Equivalent Privacy (WEP) weak or pathetic keys.

In Figure 4, 802.11 wireless network security is shown. 802.11 is a Wi-Fi wireless network communication standard and it is used in fast growing network world. It is held in 802.11 series. It operates in two different methods like Ad-hoc Networks and also infrastructure.

Figure 4: 802.11 Security



Universal Mobile Telecommunications System (UMTS) can be combined with the Wi-Fi networks for better communication purpose. The Universal Mobile Telecommunications System (UMTS) is used in the internet network world. This technology is completely dependent on the regular range. UMTS is considered as a module of the International Telecommunications Union. The previous research has already proved that the relinquish time as of the UMTS network provided to the Wi-Fi network is around 1 second to 10 seconds. In reality, Universal Mobile Telecommunications System make use of wideband rules separation many contacts.

CONCLUSION AND FUTURE WORK

In this paper, I have described about and Wired Equivalent Privacy (WEP) and Wireless Fidelity Protected Access (WPA).This kind of protections and security methods can be further more developed by the latest technologies in the world. Universal Mobile Telecommunications System can also be connected with the Wireless Fidelity (Wi-Fi) network. Through these types of networks and protocols, some of the security problems can be solved. In future, many latest technologies will be initialized and it will be very easy to tackle the forth coming Wi-Fi problems.

REFERENCES

1. Atasoy HI, Gunal, MY, Atasoy P, Elgun S and G Bugdayci (2013), "Immuno Histopathologic Demonstration of Deleterious Effects on Growing Rat Testes of Radio Frequency Waves Emitted from Conventional Wi-Fi devices", *Journal of Pediatric Urology*, Vol. 9, No. 2, pp. 223-9.
2. Djabri Fahed and Rongke Liu (2013), "Wi-Fi-Based Localization in Dynamic Indoor Environment Using a Dynamic Neural Network", *International Journal of Machine Learning and Computing*, Vol. 3, No. 1.
3. Gints Jekabsons, Vadim Kairish *et al*. (2011), "An Analysis of Wi-Fi Based Indoor Positioning Accuracy", *Scientific Journal of Riga Technical University Computer Science. Applied Computer Systems*, Vol. 47.
4. Jiangfan Feng, Yanhong Liu (2012), "Wi-Fi-based Indoor Navigation with Mobile GIS and Speech Recognition", *IJCSI International Journal of Computer Science Issues*, Vol. 9, No. 6, pp. 1694-0814.
5. Kihun Kim, Younghyun Kim, Sangheon Pack and Nakjung Choi (2011), "An SNR-based Admission Control Scheme in Wi-Fi Based Vehicular Networks", *EURASIP Journal on Wireless Communications and Networking*.
6. Li Li, Xiaoguang Hu and Baochang Zhang (2013), "A Routing Algorithm for Wi-Fi-Based Wireless Sensor Network and the Application in Automatic Meter Reading", *Mathematical Problems in Engineering*.

7. R S Deshmukh (2013), "Wi-Fi Based Vital Signs Monitoring and Tracking System for Medical Parameters", *International Journal of Engineering Trends and Technology (IJETT)*, Vol. 4, No. 5, pp. 2231-5381.

8. Tulin Mangir *et al*. (2011), "Analyzing the Impact of Wi-Fi Interference on ZigBee Networks Based on Real Time Experiments", *International Journal of Distributed and Parallel Systems (IJDPS)*, Vol. 2, No. 4.

9. Vandana Wekhande (2006), "Wi-Fi Technology: Security Issues", *Rivier Academic Journal*, Vol. 2, No. 2.