International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

Optimized De-Authentication Attack in IEEE 802.11 Networks

G. Mani Chandra, K. Raghava Rao, P.N.S.B.S.V Prasad V

Abstract*: *Wireless attacks, of late, have become the foremost threat in the field of Wi-Fi technology. This is mainly attributed to the lack of easy and affordable monitoring systems that can recognize behaviors of patterns in different attacks. MAC layer vulnerabilities are main reasons for the significant number of DDoS/DoS attacks in Wi-F access points. During the implementation of De-authentication attack, an attacker transmits a bulk of spoofed De-authenticated frames to the legitimate clients/users, which result in the disconnection from the Wi-Fi access point to which they are connected. Existing techniques of De-authentication-DoS attack rely on the encryption algorithm and protocol modifications. Nevertheless, this paper mainly focuses on the implementation of De-authentication attack in a smart way by localizing the client movement in Wi-Fi networks. In particular, we present a new attack and its experimental set up, and demonstrate its De-authentication.

Index Terms*: *RSSI, RF Localization, Wireless Intrusion Detection System, De-authentication

I. INTRODUCTION

In the recent past, Wi-Fi technology has taken over a major part of communications. Wi-Fi technology includes access points, wireless devices and end routers.

Recent advances [2] in Wi-Fi standards have made it the most effectively and widely used communication medium, both in personal and enterprise networks. The most important advantages are mobility, flexibility and low cost deployment. In addition, maintenance is easy, especially in places where deploying wired network is critical and crucial. Due to the rapid growth in the deployment of WLANs, the security issue of Wi-Fi networks has become a serious concern for clients as well as the providers.

There are three main types of [7] frameworks, viz, data frameworks, management frameworks and control frameworks. This paper mainly focuses on management frameworks, Authentication/De-Authentication, beacons, and all requested probes/response probes that are used by clients/wireless users to initialize or split sessions for network activities. Unlike data frames, these data frames can be encrypted to provide more confidentiality and security. All of these frameworks can be understood by any user and, therefore, can be transmitted as open /unencrypted. In contrast, management frames can not be encrypted, but must be protected from duplication to protect Wi-Fi devices from different types of attacks.

The first wireless standard (IEEE 802.11) has been established in 1996 [4][7]. Subsequently, there have been several revisions conducted for the improvement of the standards. Nevertheless, most of those revisions [2] have been focused on behavior and the performances of the network. IEEE 802.11i standard has been developed for providing better security to the wireless network, which provided good mechanism for improving confidentiality. This has, however, not provided enough protection for integrity. For protecting wireless protocols from vulnerabilities, it is known that all the W-IDS System and W-IPS play an important role [2][8]. These detection systems provide more security to the wireless networks by monitoring the behavior of state transitions of the protocol for detecting any type of anomalous events triggered by attacker. IDSs are classified into three different systems viz, Host based IDS, Network IDS, Wireless IDS. Even though there are many IDS/IPS systems which are available for wired networks, these cannot be deployed directly into the network. Most of the IDS/IPSs operate on the Physical and Mac layers.

In our study, we have discovered new attack which is a bit different from all existing De-authentication-attack approaches built on the wireless networks. By launching such type of attack, the adversary cannot be detected by IDS.

Our smart attack devastates the WPA and also WPA-2 supplicant and Wi-Fi users commonly connecting to the access point. Most of the mobile devices and the access points use modified WPA-Supplicant. In a recent survey [2][7], it has been found that around 31.2 % of latest smart devices are vulnerable to De-authentication attack. Interestingly, we have never changed/modified any security properties of the wi-fi target device for implementing attack. The core contributions of the present work may be summarized as follows:

- We have introduced a new method of attacking the Wi-Fi access points which is different from the existing way's in the implementation of the attack.
- We have evaluated the practical impact of this attack on the network before and after launching the attack.

This paper is organized as several sections. Section 2 describes basic Literature survey. Section 3 presents the attack setup. The paper concludes with Section 4, which discusses the conclusion and future scope of this project.

Revised Manuscript Received on 30 March 2019.
***** Correspondence Author
G. Mani Chandra*, Department of ECM, Koneru Lakshmaiah Educational Foundation, Vijayawada, India..
P N S B S V Purna V, Master's Student, Department of ECM, Koneru Lakshmaiah Educational Foundation, Vijayawada, India.
K Raghava Rao, Professor, Department of ECM, Koneru Lakshmaiah Educational Foundation, Vijayawada, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

II. LITERATURE SURVEY

This section introduces basic survey on IDS and IPS.

A. Types of Attacks

In what follows we describe in brief various types of attacks and their implications.

I. PHYSICAL ATTACKS:

Physical attacks target the bottom Layer (physical) as well as Hardware and Software of Machine to Machine Devices. Some of the attacks **[4][6]** that come under this category are Side Channel Attack, Software Modification and Malwares, to name a few.

Side Channel Attacks:

In general, all the Machine to Machine devices are placed in nearby locations where attackers can easily access and exploit them for performing side channel attack. Mostly these types of attacks are based on power consumption and timing information and enable the retrieval of the used. For example, an attacker may conduct a side channel attack on any of the client device for retrieving the keys which are used for Encryption/Decryption of exchanged data between client and server.

Software Modification and Malwares:

In order to alter the proper operations of the machine to machine device [4], Software modifications are, in general, performed by an adversary, or even a genuine client in the network, Malicious users may do it in order to reduce the amount of the charges which they have to pay. For example, such a misbehaviour may be noticed when smart metering or eToll applications are dealt with. These attacks are also conducted even without direct access to the device since all the software updates are performed Over-The-Air (OTA). The impact of this type of attack is very high in such scenarios as electronic Health or mechanical applications, when everything remains under the control of attacker.

II. LOGICAL ATTACKS:

Logical attacks target the proper functions of the System without making any changes to the client Device Software. This category attacks include Impersonation, Denial (or Distributed)-of-Service attack, Relay attack.

Impersonation:

This attack is due to the possibility of an attacker spoofing the credentials of the device/access point/gateway. This attack could turn out to be very dangerous in the sense that it has potential to lead to the financial as well human losses. For instance, the adversary who is successful in spoofing the smart device credentials can make its owner pay for the attacker's charges. In worst case, the attacker may even impersonate the device as he would be able to transfer control functions to the corresponding devices/gateway. For example, in the case of electronic health application, this attack can pose a threat to normal/abnormal human life.

Denial of Service (DoS):

As most of the wireless devices work on battery power, the continuous broadcast of unknown data packets drain the battery, which results in the failure of application [3][2][7]. These attacks are conducted by attackers to disconnect legitimate users from the access points. This type of attack causes unavailability of resources to the client(s) in the network, and also leads to substantial financial losses in majority of applications.

Relay Attacks:

This attack [2][3] includes the possibility of an attacker making the system/device/gateway believe that it is under vicinity of the transceiver. This type of attack may also target the device/ gateway, or entire network. For example, there is a possibility that this relay attack can be inflicted when dealing with the Electronic Toll application for forwarding the payment request to a driver who is the owner of the vehicle. As a result, the owner is made to pay additional amount for the journey that he never took.

III. DATA ATTACKS:

These attacks normally target exchanged information between many devices. The attacks that come under this category are privacy attacks, injecting false/modified data and interception, to name but a few.

Privacy Attacks:

Because of all pervasive wireless devices [6][11], attacker can invade users' privacy policy and link up the wireless devices to individuals by gaining information about users' habits and health condition. In this process, attacker eavesdrops exchanged packets that consist of huge data [4]. Let us consider an example that there is a possibility that the adversary may know that he/she is the owner who suffers from heart problem. In some applications like PAYD insurance and electronic tolling, the localized information is sent to the administrator who provides all the services for tracking the details of user's destiny.

Injecting false\modified data:

This includes the possibility of data being compromised during the transmission between device to device. For instance, let us consider the case of electronic health/e-Call applications [11]. In view of the modification being done to the measured values of data or localization information, there is endanger to human life. Further, in some applications, injection of false data may result in financial losses.

Interception:

This type of attack is conducted against the developing infrastructure like the network domain, but they can also be carried away against the network gateway.

B. Intrusion Detection System:

Due to the proliferation of e-commerce and dependence on internet, it is of importance to detect and prevent DoS attacks timely. Wireless Intrusion Detection Systems (WIDSs) [22] are designed for this purpose. A WIDS is an open source software tool which works on any Linux environment. For example Wireshark is used to sniff the network data for retrieving suspicious activities in the network. Some of its purposes are mentioned below:

Detection of mass De-authentication frames which are sent to legitimate clients for handshake.

1) Continues sending of data to access point using broadcast Message-Authentication-Code address which indicates the possibility of wireless attacks.
2) Involvement of less amount of data communication between wireless user/client and access point using Extensible Authentication Protocol (EAP) authentication which indicates the possibility of Sync Flooding attack.

WIDSs [2] are broadly categorized into two, according to their reference data or behavior analysis techniques. As per the reference data, the Wireless IDSs can be grouped into three groups, viz, those which focus on the data in physical layer, MAC layer data and the others which combine the attributes of both layers.

According to analysis technique, WIDS can be classified into misuse detection and anomaly detection. IDS is a system application which is used to provide security against different wireless attacks.

The two main functions used in identifying De-authentication attacks using WIDS are monitoring the incoming packets and logging the information of packets. WIDS not only detects the De-Authentication attack, but also singles out a fake AP on the Wireless Network by randomly comparing MAC address with Authorized AP MAC address and capturing the de-authentication frames consisting of BSSID, DA, SA, reason code and frame control.

Detection of de-authentication attack [22] using WIDS (analysis technique) is classified into three approaches. These are signature based approach, anomaly based approach and specification based approach. Signature based detection [8] is one of the methods of detection which utilizes the signatures collected in a database. These signatures have different patterns that are pre-configured and predetermined. A signature-based IDS/IPS monitors all the network traffic to generate signatures. All the generated signatures normally have some pattern. IDS matches these generated patterns to the normal patterns in the database or memory. If patterns with abnormality are found during the process of matching, then intrusion prevention system takes immediate action on these detected intrusions [18]. Signatures are generated based on vulnerability analyses using all the vulnerabilities in a script. In this approach, all the frames of data which have been transmitted over the network will be captured and compared to the data in a database SQL format. If any false data is detected, an alert signal will be generated to the user for the prevention. If the intruder transmits some unknown data, typically this detection approach fails to detect the attack [22]. Signature detection approach is more successful in detecting known attacks, but are not so good in detecting unknown attacks.

The authors of [14] have proposed new methodology which is based on entropy for distinguishing the false positives and false negatives of IDS. In addition, they have presented the vulnerabilities of monitoring devices using the concept of entropy.

C. Wireless Intrusion Prevention System

WIPS [21] is a complex security device or integrated software application which is used to monitor and detect the radio spectrum of malicious access points and also other wireless threats which are surrounded in the specific area [17].

IPS compares all the signatures in the database to BSSID of all wireless access points in the network. If IPS detects any suspicious data, the administrator gets alerted. For detecting spoofed BSSID of device, IPS systems are available for analyzing the signatures of access points which are unique.

The PCI Security Standards Council recommends the usage of WIPS to scan the wireless networks automatically [1][21]. Besides providing the security for wireless LANs, IPS is also used to monitor performances of network and discovers wireless access points which have configuration errors by default.

Integration of WIPS into network is classified as three methods. They are as follows[17]: The first method is time slicing or time-sharing. In this type of arrangement [17], the Wi-Fi devices play a double role in performing duty, providing network data to wireless connections while periodically scanning for unauthorized access points. In the Second method (Integrated IPS) [19] an inbuilt sensor in access point is deployed by manufacturers for continuously scanning signatures of nearby radio frequencies to detect fake access points. The IPS-overlay is the third method. In this method, all the sensors are deployed throughout a building for capturing RF Signals of surrounded Wi-Fi access points. All these IPS sensors collect the data and transmit the same data to a centrally authorized server for further analysis of intrusion, action and log archiving. This method is highly expensive as it requires more dedicated hardware, but is most effective for prevention. The hardware of IPS-overlay requires backend server and associated sensors which resemble wireless access points. Most of the IPS-overlay systems share fundamental components like sensors, management server, database server, console to provide the interface to administrators for setting up and managing the Intrusion prevention system.

These are hardware/software network security appliances which are used for the purpose of monitoring network for detecting abnormalities in network data [18]. IPS logs all the information of activities and attempts to block/reject activities if it detects any error in packet and reports those recorded activities to administrator. These can be placed in-line to prevent intrusions which are detected. Moreover WIPS [9] takes action after alerting the administrator by sending alarm signals, dropping of defective packets, resetting/removing the connections. An IPS can also correct Cyclic/Frame Redundancy Check (CRC/FRC) errors, de-fragment packet data, prevention of TCP sequence issue and cleaning the unwanted transport as well as network layer options.

Intrusion prevention systems can also be classified as:

1) A Network Intrusion Prevention System:
   This system is used for monitoring the entire network for suspicious traffic by analyzing networking activities [15][17].
2) Wireless Intrusion Prevention Systems:
   It monitors all the wireless networks for suspicious activities in traffic data by analyzing the wi-fi network protocol [23].
3) Network Behavior Analysis Method:
   This method is used to examine all the network traffic for identifying threats that generates DDOS attacks and network policy violations.
4) Host Based Intrusion Prevention System:
   It is a software package that is used to monitor single host for identifying/determining suspicious activities by analyzing those events that occur within the system (host).

III. ATTACK SETUP

In this section we describe the new attack that we have generated and provide experimental setup in detail. In our experiment, we have mainly focused on the implementation of de-authentication in a different way. To begin with, we have considered four mobile access points (within short distance) and monitoring devices. In this set up, monitoring device extracts all the information of all the clients that are connected to access point. All these access points are the major players in the market today. Using Wireshark tool, we have then captured the communication between the client and access point including probe requests. A probe request is a frame sent to access point by a user device. User device requests information from either a specific access point, specified with name or BSSID (MAC Address) or all access points in the surroundings. Capturing of these probe request/response packets is done to get information about client who wants to get connected to the access point. All the BSSIDs with signal strength from nearby access points are monitored using monitoring device. Monitoring device sends the same information to attacker.
We have shown the experimental setup in Figure 3.

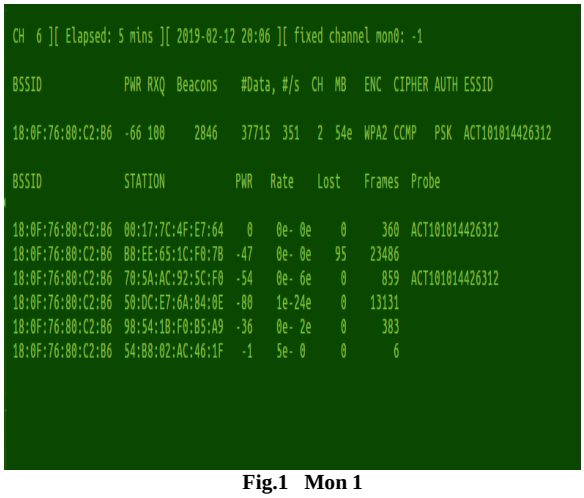

Fig.1 Mon 1

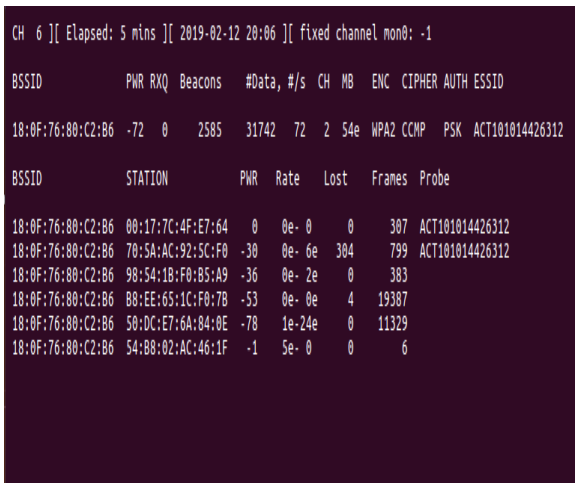

Fig.2 Mon2

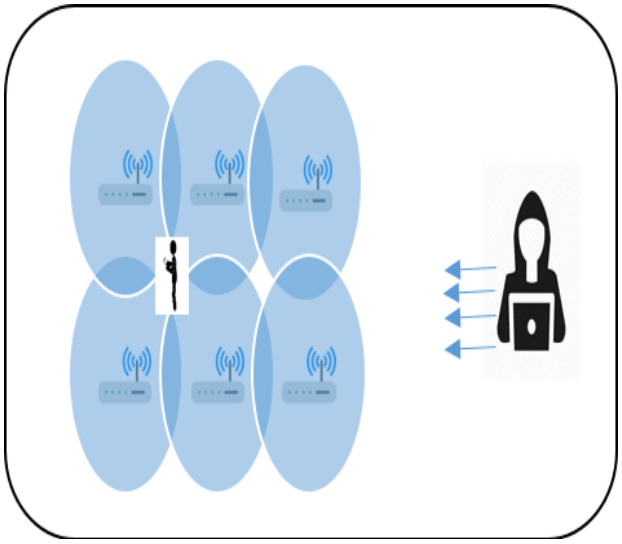

Fig.3 Attack Setup

IV. ATTACK ENVIRONMENT

For attacking the access point(s) we need to consider:

- Commodity Wi-Fi module, enabled with Rf monitoring mode for retrieving received signal strength information [16].
- Set up access point(s) so that client can be connected for the resources.
- Set up an attacking device which is in the coverage region of access point.
- Floor map of the indoor area.

Our smart attack has been performed on the Wi-Fi access point as mentioned above in Section III. During the process of de-authentication attack on the surrounding access points, the users connected to access point are unable to utilize the network resources. Thus attacker will be denying the service. Our method of attacking the access point has been successful on all Wi-Fi devices that are placed in corridor. Our experiment has been conducted in Department corridor, IIT-H Campus (Figure 4).

Fig.4 Department corridor (IIT-Hyderabad)

For the simulations, we have considered a trained set of data which is random RSSI value and distance. We now report our results in terms of several figures. To begin with, we have shown the information from the 1st and 2nd monitoring devices (Mon 1 and Mon 2) in Figure 1 and Figure 2 respectively. From the Figure 7, we can clearly observe that the received signal strength is inversely proportional to the distance between client device and Wi-Fi access point.

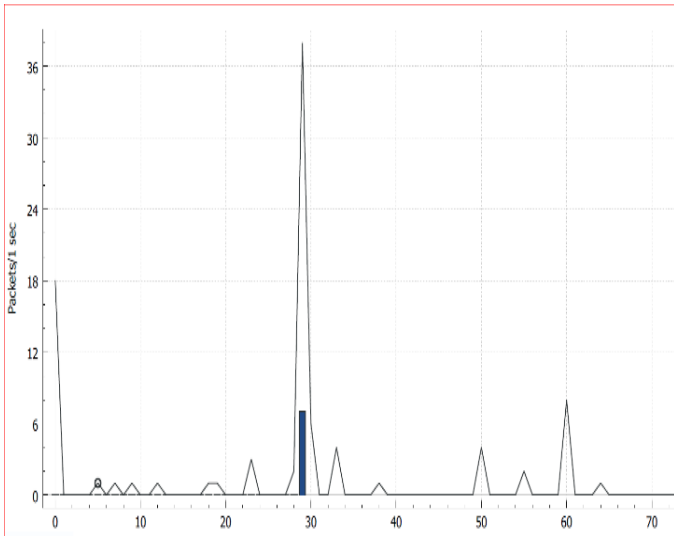

Fig.5 Network Performance during Attack

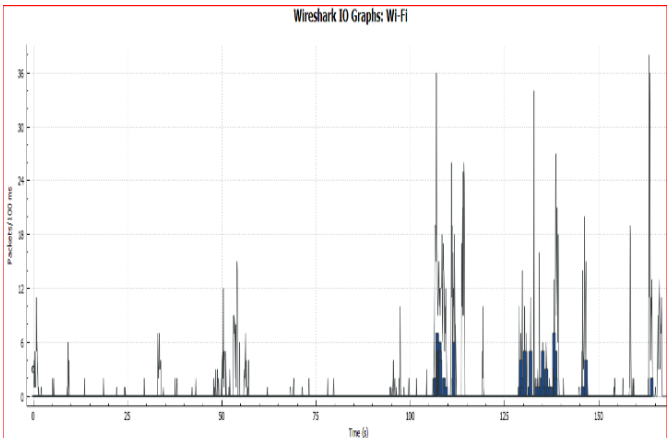

Fig.6 network Performance before Attack

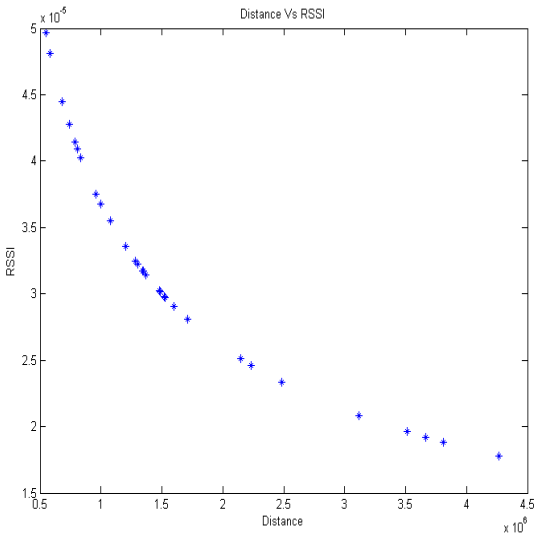

Fig.7 Distance Vs RSSI

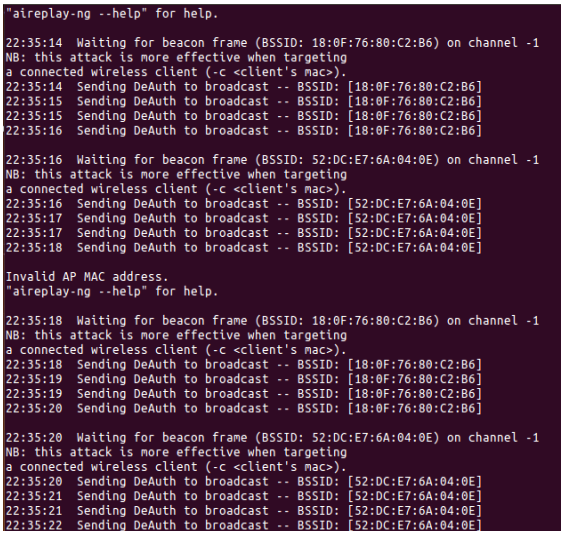

Fig.8 De-Authentication Attack

V. CONCLUSION AND FUTURE SCOPE

In this paper, we have presented De-authentication attack that has been done on dual-band hardware (Wi-Fi access point) in a smart way by localizing the client connected to the Wi-Fi access point. Further, we have also addressed the problem of estimating location of client with moderate accuracy using RSS Information. The impact of our methodology in attacking depends on number of clients connected to access point. The salient features of our method is that the attack is economical and its set up is easy. The counter measurement that we have considered for this attack is RSS (Received Signal Strength) information of device from multiple monitoring devices and also fingerprint map of location. Experimental results have shown that our methodology has raised the indoor localization accuracy. Accuracy could be further improved by using channel state information which is retrieved from physical layer data and by deploying more monitoring devices within short distance. This approach can further be extended to three dimension by including the Z-coordinate. But in this case, minimally fourmonitoring devices are required for a unique solution indoors.

ACKNOWLEDGMENT

One of the authors (Mani Chandra) is grateful to Prof. Abhinav Kumar, Indian Institute Of Technology, Hyderabad for helpful discussions.

REFERENCES

1. Available at https://www.pcisecuritystandards.org
2. Hamid Alipour, Youssif B. Al-Nashif, Pratik Satam, and Salim Hariri, Member, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 10, OCTOBER 2015.
3. https://blog.ct-networks.io/types-of-wireless-attacks-9b6ecc3317b9
4. Barki, Amira, Abdelmadjid Bouabdallah, Said Gharout, and Jacques Traore. "M2M Security: Challenges and Solutions", IEEE Communications Surveys & Tutorials, 2016
5. Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, “Home M2M networks: Architectures, standards, and QoS improvement,” IEEECommun. Mag., vol. 49, no. 4, pp. 44–52, Apr. 2011.

6. Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, “Privacy in machine-to-machine communications a state-of-the-art survey,” in Proc.IEEE Int. Conf. Commun. Syst. (ICCS), Nov. 2012, pp. 75–79.
7. Available at Wikipedia.org Shashank Khandelwal, Parthiv Shah, Mr. Kaushal Bhavsar, Dr. Savita Gandhi,'Frontline Techniques to Prevent Web Application Vulnerability',International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)Volume 2, Issue 2, February 2013
8. Detection and Mitigation DDoS Defence Techniques to Strengthen Intrusion Prevention Systems,"V.Suresh 1 , Dr.A.Rajiv Kannan 2 , K.Sudhakar 3
9. Flitz,http://www.packetstormsecurity.org/distributed/flitz-0.1.tgz
10. "Analysis of Security Vulnerabilities for Mobile Health Applications","Y. Cifuentes, L. Beltrán, L. Ramírez".
11. https://wtf.horse/2017/10/02/introducing-nzyme-wifi-802-11-frame-recording-and-forensics.
12. https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame.
13. "Deceiving entropy based DoS detection" Ilker Ozc € ¸elik*, Richard R. Brooks Holcombe Department of Electrical and Computer Engineering Clemson University, Clemson, SC 29634-0915, USA
14. A. H. Al-Hamami and G. M. W. Al-Saadoon, "Development of a network-based: Intrusion Prevention System using a Data Mining approach," 2013 Science and Information Conference, London, 2013, pp. 641-644.
15. https://www.cnet.com/products/intel-ultimate-n-wifi-link-5300-network-adapter-series/.
16. Stiawan, Deris and Yaseen, Ala and Idris, Yazid and Abu Bakar, Kamarulnizam and Abdullah, Hanan,"Intrusion prevention system: A survey"2012, 44-54,Journal of Theoretical and Applied Information Technology.
17. https://www.vskills.in/certification/tutorial/basic-network-support/intrusion-detection-and-prevention/
18. https://whatis.techtarget.com/definition/WIPS-wireless-intrusion-prevention-system
19. https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/
20. David D. Coleman, David A. Westcott, Bryan Harkins. "CWSP®: Certified Wireless Security Professional Study Guide CWSP-205", Wiley, 2016.
21. Elhadj Benkhelifa, Thomas Welsh, Walaa Hamouda. "A Critical Review of Practices and challenges in IDS for IoT: Towards Universal and Resilient Systems", IEEE Communications Surveys & Tutorials, 2018.
22. Available @ www.uniascit.in