A novel algorithm to detect Man in the Middle Attack in WLANs

Rajinder Singh, Satish Kumar

Abstract: *Wireless local area networks (WLANs) are growing very rapidly in recent years. With the growing popularity of the wireless network, risk of security attacks associated with wireless network is also growing. Access Points (AP) are used in many public places like airport and hospitals to provide the users internet facility. Due to the open nature of the wireless networks, it is vulnerable to many different types of threats. Main wireless threats are eavesdropping, man in the middle attack and evil twin attack etc. In this paper one such threat MITM (Man in the Middle Attack) is discussed. In this case attacker creates a Rogue Access Point (RAP) using the same parameters as that of original AP of the network, with the help of software. We propose a methodology to detect the MITM attack. Our algorithm use combination of RSSI (Received Signal Strength Indicator) value and sequence number for detecting this attack.*

Keywords: MITM, RAP, RSSI, RTT

I. INTRODUCTION

Wireless networks are growing rapidly. Main advantages of using wireless networks are portability, flexibility and ease of using. But with the growth of wireless network risk of security attacks are also growing rapidly. Security of wireless network is a great concern for many years. Due to the broadcasting nature of the WLAN, it is vulnerable to many threats [1]. One common threat to the wireless network is rogue access point. A rogue access point is a fake access point installed by an attacker to sniff the wireless network traffic. Main attention of the attacker is to harm the business of the organization. It is a very common method used by the attacker to intercept the sensitive and confidential data. A rogue access point can also used to carry out the MITM attack. It is very simple and inexpensive to setup a rogue AP [2]. Main threats which are caused by the MITM attack are highlighted below. Data Theft: One use of MITM attack is intercepting information related to organization. By passive sniffing an attacker is able to get the information related to network users. Attacker is able to get the information related to user's IP address. In some cases where the network is poorly configured attacker can steal sensitive information such as username and passwords. Free Internet: Once MITM attack is successful, attacker can use the organization's Internet facility at free of cost. It can also be used for criminal purposes. DoS Attack: RAP can be used by the attacker to flood the network with useless packets. It can also launch DoS attack to bring down an organization's network. Main examples of DoS attacks are ARP poisoning, Session Hijacking and IP spoofing [3]. There are many tools available over the Internet for launching such kind of attacks. Email Hijacking: With the help of MITM attack an attacker can also target email accounts of a financial organization. If an email account is hijacked, attacker can monitor the detail of a transaction. Session High-jacking: With the help of this attack, an attacker can hijack the session. Attacker can steal the cookie. Cookies are small piece of information that makes the web browsing easy. It contains useful information such as location, login credential or any online activity. If an attacker is able to get the login cookie, then he or she can log into the account and can take user's identity [4]. Therefore, a RAP is a very serious threat to the network security.

Revised Manuscript Received on August 30, 2019.

* Correspondence Author

Rajinder Singh*, DCSA, Panjab University SSGRC, Hoshiarpur, Punjab, India. Email: rajinderid@gmail.com

Dr. Satish Kumar, DCSA, Panjab University SSGRC, Hoshiarpur, Punjab, India. Email: satishnotra@yahoo.co.in

II. PROBLEM STATEMENT (MAN IN THE MIDDLE ATTACK)

In a wireless network, AP is used to connect the clients to the local area network. It can be connected to the server through wires or without wires. AP is used to transmit data between the client and network. In a normal scenario (Fig.1) it is clear that client is directly connected to AP. But in case of MITM attack attacker insert himself/herself between the valid AP and user. Therefore attacker is able to intercept data, receive data and send it back. Attacker can also modify data before sending it to the network.

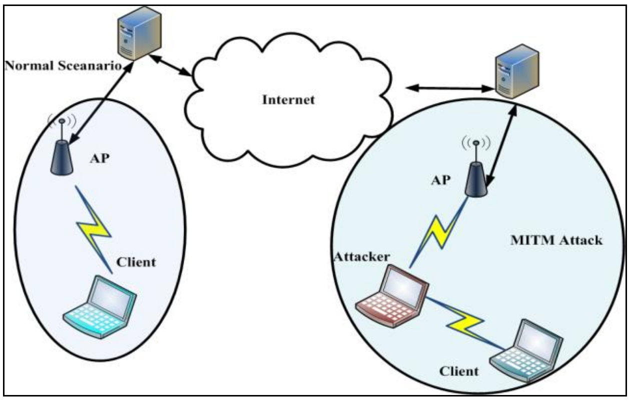


Figure 1. MITM Attack.

III. LITERATURE REVIEW

In paper [5] authors analyzed this attack with the help of mathematical model. Then they gave the relationship between the two communicating nodes and the attacker. They analyzed the relationship among these with the help of mathematical logical operations and propositions. This model tells whether a given system is vulnerable to this attack or not. They also suggested a defence model to remove the vulnerabilities. In paper [6] authors discussed MITM attack when there is internetworking between 3G network and WLAN network. They discussed the vulnerability present in the gateway which is used to transfer the protocol. Packets are vulnerable during the protocol transfer. Authors in the paper [7] gave a practical method to determine whether a given user is connected to an authorized access point or not. They used client devices for scanning rogue access point. They proposed that this method can detect evil twin attack as well as MITM attack. According to authors [8] Transport layer Security (TLS) is main building block for network security and it is used in virtual private networks. Here main procedure is authentication and key exchanging. But insecure keys can lead MITM attack in VPN also. Authors [9] proposed a novel method to detect MITM attack. They analyzed Round Trip Time and Received Signal Strength. Then they used statistical measures to detect the MITM attack. But limitation of this method is that RTT values and RSSI values can be affected by many other parameters. Han et al. [10] have proposed client centric approach for detecting RAP. It uses Round Trip Time (RTT) between DNS server and user for checking RAP. Limitation of this approach is RTT can be affected by many factors such as location of DNS server, data transmission rates, interference from other packets which can change the RTT values. Yang et al. [11] have proposed Evil twin access point detection technique from user side. Authors proposed two statistical anomaly detection algorithms, Training Mean Matching (TMM) and Hop Differentiating Technique (HDT). This method is time consuming. The trained knowledge of one network is not applicable to another network. Further this method will not work properly if remote servers are not available. Kim et al. [12] have proposed a method which use received signal strength (RSS) values. These values are normalized for getting accuracy. Main limitation of this method is that it only focuses on moving client devices. Gajbhiye et al. [13] have proposed cluster analysis of RSS values for detecting the spoofing attack. Authors used Mean Shift algorithm for cluster analysis. L. Rahman et al. [14] have proposed SALT-HASH algorithm for detection of MITM attack. But limitation of this method is that it is applicable only after exchanging SALT messages. Zhanyong Tang et al. [15] proposed a method to detect MITM attack in case of smart homes. They also used RSSI values for the detection of this attack. Authors [16] proposed a method which uses sequence number for detecting the MITM attack.

IV. ARCHITECTURE

The test bed for the MITM attack is shown in Fig. 2. In this study test bed consist of wireless network, an AP, a client device and an attacker machine. A server for monitoring and scanning wireless traffic is also used. Initially attacker scans the wireless packets for gaining important information of clients, wireless traffic and access points and launches the MITM attack.

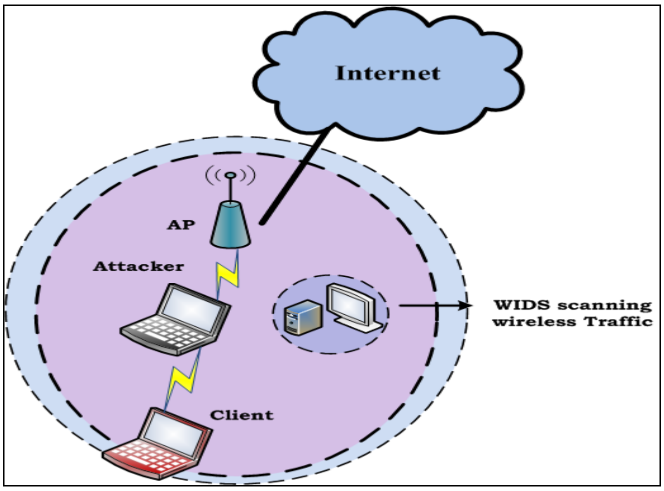


Figure 2. Test Bed for detection of MITM Attack.

V. RESEARCH METHODOLOGY

A. Design

The system has two modules- i) For computing average strength of packet sent by the original access point and ii) for detecting the rouge access point in the monitoring area (Fig. 3). The system has a packet queue that captures all the packets in the area and insert into the queue. Initially when the system is turned on, the strength computing module will start and it collects packets to detect the signal strength of the given network in the form of various parameters. After acquiring the information, the system starts its detection module for intrusion detection on the system. There are two methods for RAP detection: i) Access Point with same SSID but different MAC. ii) Access Point with same SSID and MAC address. Detection of the first attack is easy as you can capture the packets and easily scan for the threat. For second type of attack, the system uses two parameters; one is packet sequence number and second is packet signal strength. The sequence number of fake AP in most cases will generate the sequence number that will not match with the original AP's sequence number and the system check for the arbitrary number in sequence to detect that. If the attacker manages to change the sequence number to the original one, the system will detect attack on the basis of signal strength as for a successful attack, the signal strength of fake AP has to be greater than the original AP.

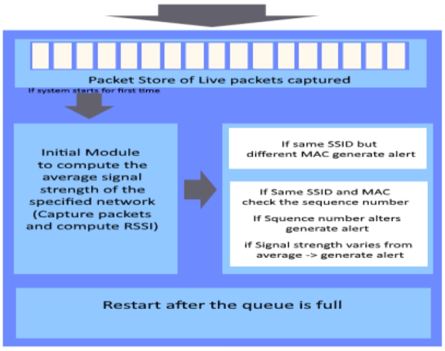

Packet Store of Live packets captured
If system starts for first time
Initial Module to compute the average signal strength of the specified network (Capture packets and compute RSSI)
If same SSID but different MAC generate alert
If Same SSID and MAC check the sequence number
If Squence number alters generate alert
if Signal strength varies from average -> generate alert
Restart after the queue is full

Figure 3. Research Methodology.

B. Working

When the WIDS starts operating, it starts capturing all the 802.11 frames and dissects and inspects the packets. Along with these tests the WIDS also maintains the logs of these packets for future studies. It also keeps track of all the neighboring BSSID, SSID, RSSI values and Channel number. If the WIDS detects an attack during scanning it generate alerts and maintains the details in the LOG files.

C. Detection of Attack

Main parameters which are considered in our algorithm for the detection of this attack are i) Sequence Number ii) Signal Strength i) Sequence Number : When a packet comes from a higher layer to MAC layer, a sequence number is given to the packet. If an in- coming packet is very big then it is split into multiple parts called fragments, and a fragment number is given to fragment number field. Fragmented frames contain same sequence number with different fragmented value [17]. ii) Signal Strength: RSSI value is a received signal strength value indicator, which tells how well client device can receive signal for the near access point. If this value is good enough then there is good wireless connection [18].

VI. RESULTS AND DISCUSSIONS

In normal case when there is no attack on the network, there is change in the sequence value as the new packet comes into the network (Fig. 4). But in case of attack mode there is no change in the sequence number value of the incoming packets. As shown in the Fig. 5. As the new packets are coming into the network there is change in the frame value of the packets but the sequence number of each new packet remains the same.

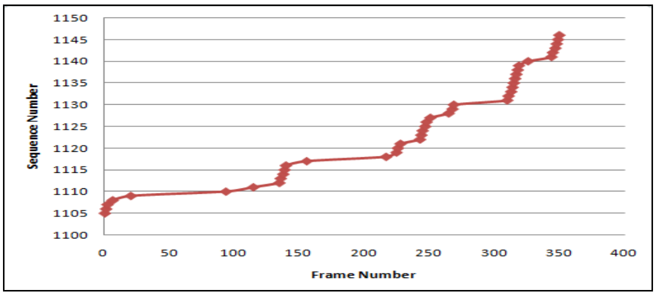


Figure 4. Change in sequence number with frame number.

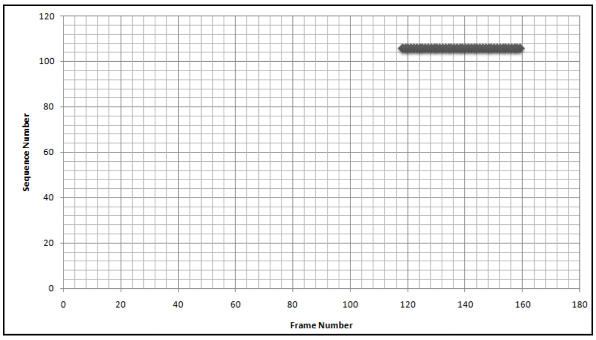
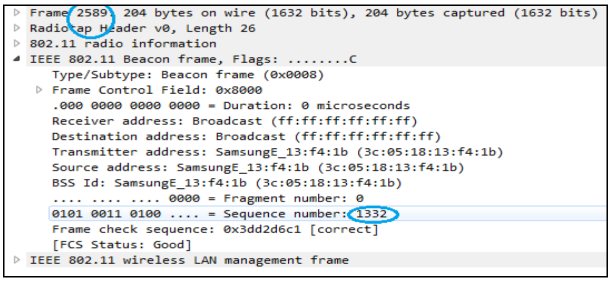


Figure 5. No Change in sequence number in MITM attack.

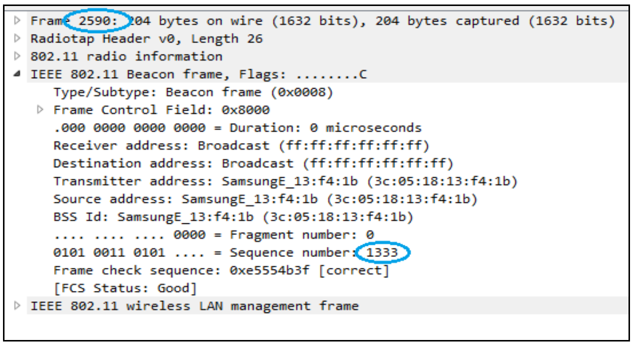
Fig. 6 given below shows the frame number and its sequence number of a captured packet.



```
▷ Frame 2589: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
▷ Radiotap Header v0, Length 26
▷ 802.11 radio information
◢ IEEE 802.11 Beacon frame, Flags: ........C
     Type/Subtype: Beacon frame (0x0008)
   ▷ Frame Control Field: 0x8000
     .000 0000 0000 0000 = Duration: 0 microseconds
     Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
     Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
     Transmitter address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     Source address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     BSS Id: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     .... .... .... 0000 = Fragment number: 0
     0101 0011 0100 .... = Sequence number: 1332
     Frame check sequence: 0x3dd2d6c1 [correct]
     [FCS Status: Good]
▷ IEEE 802.11 wireless LAN management frame
```

Figure 6. Frame Number and Sequence Number.

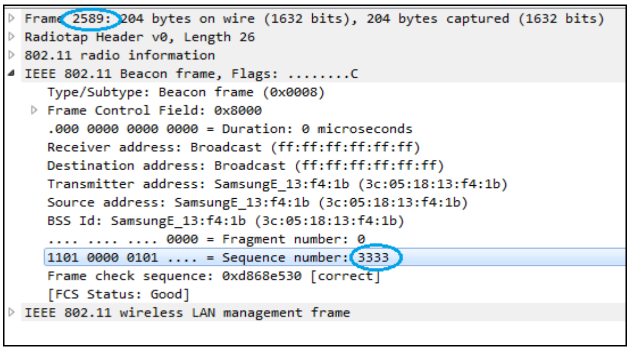
Fig.7 shows the next frame with sequence number.



```
▷ Frame 2590: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
▷ Radiotap Header v0, Length 26
▷ 802.11 radio information
◢ IEEE 802.11 Beacon frame, Flags: ........C
     Type/Subtype: Beacon frame (0x0008)
   ▷ Frame Control Field: 0x8000
     .000 0000 0000 0000 = Duration: 0 microseconds
     Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
     Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
     Transmitter address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     Source address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     BSS Id: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     .... .... .... 0000 = Fragment number: 0
     0101 0011 0101 .... = Sequence number: 1333
     Frame check sequence: 0xe5554b3f [correct]
     [FCS Status: Good]
▷ IEEE 802.11 wireless LAN management frame
```

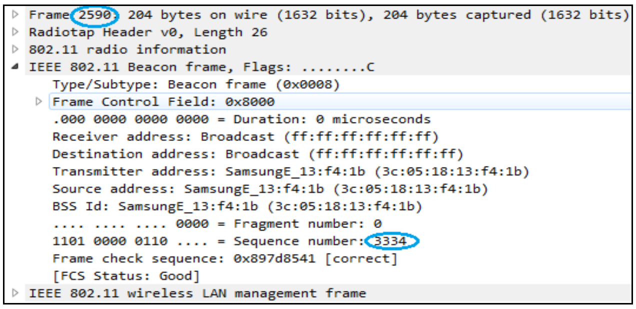
Figure 7. Frame Number and Sequence Number of Next Frame.

But nowadays a number of free tools are available on the Internet with which attacker can change the sequence number of the captured packet. Changed Sequence number of these frames is shown in Fig.8 and Fig.9.



```
▷ Frame 2589: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
▷ Radiotap Header v0, Length 26
▷ 802.11 radio information
◢ IEEE 802.11 Beacon frame, Flags: ........C
     Type/Subtype: Beacon frame (0x0008)
   ▷ Frame Control Field: 0x8000
     .000 0000 0000 0000 = Duration: 0 microseconds
     Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
     Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
     Transmitter address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     Source address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     BSS Id: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     .... .... .... 0000 = Fragment number: 0
     1101 0000 0101 .... = Sequence number: 3333
     Frame check sequence: 0xd868e530 [correct]
     [FCS Status: Good]
▷ IEEE 802.11 wireless LAN management frame
```

Figure 8. Frame Number and Changed Sequence Number.



```
▷ Frame 2590: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
▷ Radiotap Header v0, Length 26
▷ 802.11 radio information
◢ IEEE 802.11 Beacon frame, Flags: ........C
     Type/Subtype: Beacon frame (0x0008)
   ▷ Frame Control Field: 0x8000
     .000 0000 0000 0000 = Duration: 0 microseconds
     Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
     Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
     Transmitter address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     Source address: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     BSS Id: SamsungE_13:f4:1b (3c:05:18:13:f4:1b)
     .... .... .... 0000 = Fragment number: 0
     1101 0000 0110 .... = Sequence number: 3334
     Frame check sequence: 0x897d8541 [correct]
     [FCS Status: Good]
▷ IEEE 802.11 wireless LAN management frame
```

Figure 9. Changed Sequence Number of Next Frame.

Therefore considering this parameter alone is not sufficient for detecting this attack. Some algorithm use RSSI value for the detection of RAP. But problem with RSSI value is that it can be changed by a number of factors e.g. interference, noise or home appliances. In normal scenario graph between RSSI value and Sequence number is shown in Fig.10. From the graph it is clear that the RSSI value of the AP remains mostly -64 dBm.

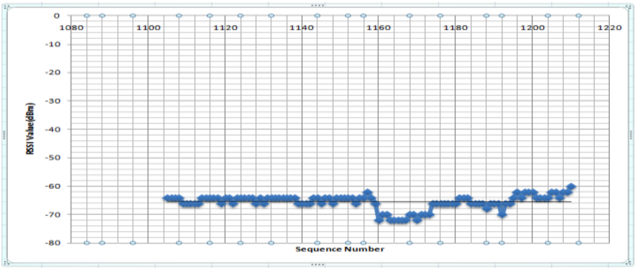


Figure 10. RSSI value of a valid AP.

Fig. 11, 12, and 13 shown below show the change in the RSSI values due to air. These snapshots are taken from the same location. Fig. 11 shows a number of AP active within the same location.

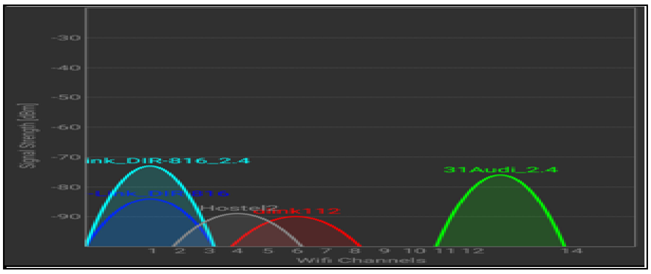


Figure 11. RSSI value of valid APs within a location.

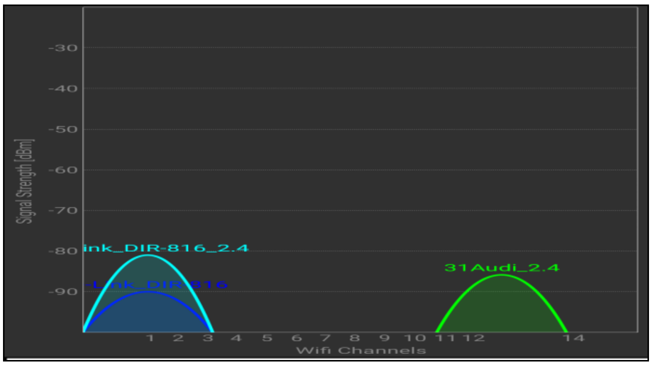


Figure 12. Change in RSSI values of AP.

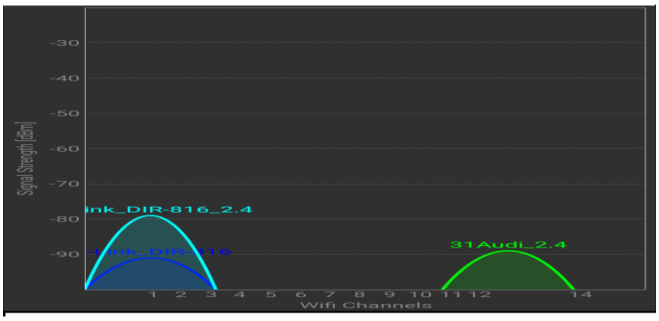


Figure 13. Change in RSSI values.

Fig. 12 and 13 shows the change in the RSSI values of valid APs due to the air. Therefore sequence number alone or RSSI value alone cannot be used to detect the RAP as it will increase the number of false positive. So we suggest a new algorithm which will use the combination of these two values. Flowchart of the suggested algorithm is given below (Fig.14).

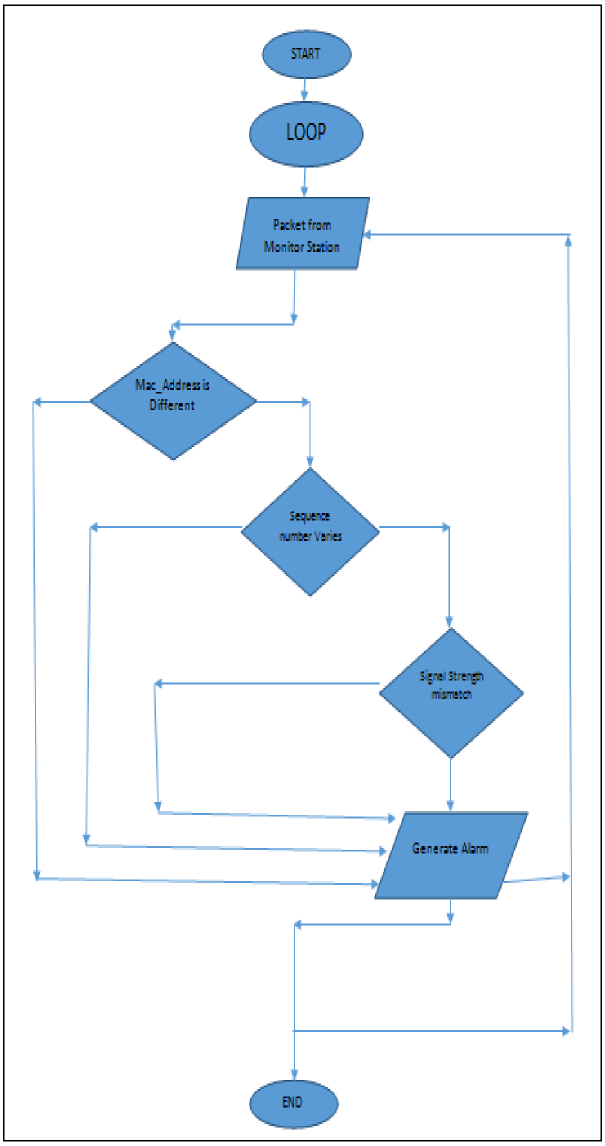
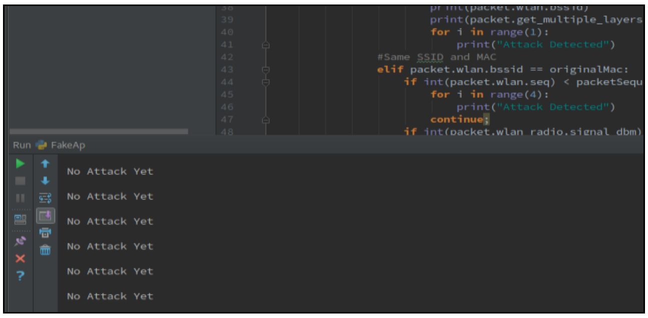


Figure 14. Flowchart for the proposed solution

Extensive experiments are conducted to study the behavior of nodes under normal as well as under MITM attack conditions.

We have tested our algorithm for five clients and it successfully detected the MITM attack. Result of detecting the MITM attack using our algorithm is shown in Fig. 15, 16 and 17. Fig.15 shows the result of our algorithm when there is no attack on the network.

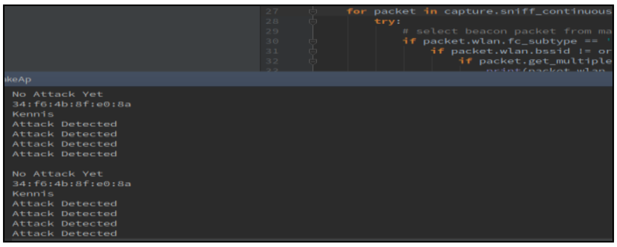


```
                print(packet.wlan.bssid)
                print(packet.get_multiple_layers
                for i in range(1):
                    print("Attack Detected")
        #Same SSID and MAC
        elif packet.wlan.bssid == originalMac:
            if int(packet.wlan.seq) < packetSequ
                for i in range(4):
                    print("Attack Detected")
                continue;
            if int(packet.wlan radio.signal dbm)
```

```
No Attack Yet

No Attack Yet

No Attack Yet

No Attack Yet

No Attack Yet

No Attack Yet
```

Figure 15. When there is no MITM attack.

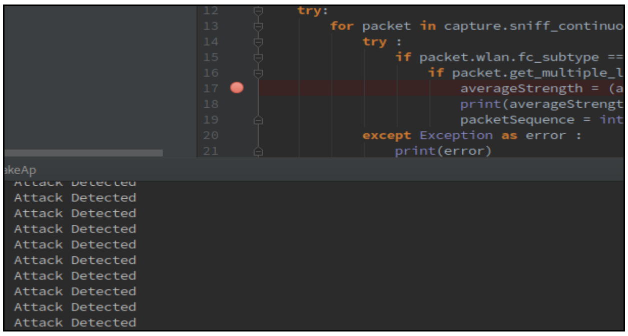
Fig.16 and Fig.17 shows the result in case of MITM attack.



```
        for packet in capture.sniff_continuous
            try:
                # select beacon packet from ma
                if packet.wlan.fc_subtype == '
                    if packet.wlan.bssid != or
                        if packet.get_multiple
```

```
No Attack Yet
34:f6:4b:8f:e0:8a
Kennis
Attack Detected
Attack Detected
Attack Detected
Attack Detected

No Attack Yet
34:f6:4b:8f:e0:8a
Kennis
Attack Detected
Attack Detected
Attack Detected
Attack Detected
```

Figure 16. When there is MITM attack on one client device.

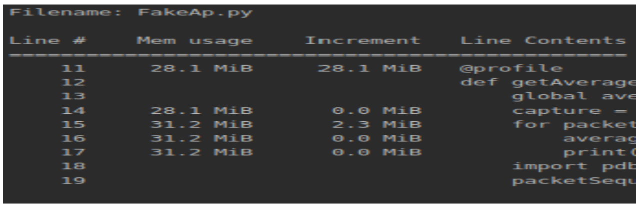


```
    try:
        for packet in capture.sniff_continuo
            try :
                if packet.wlan.fc_subtype ==
                    if packet.get_multiple_l
                        averageStrength = (a
                        print(averageStrengt
                        packetSequence = int
            except Exception as error :
                print(error)
```

```
Attack Detected
Attack Detected
Attack Detected
Attack Detected
Attack Detected
Attack Detected
Attack Detected
Attack Detected
Attack Detected
```

Figure 17. MITM attack on the other client.

Memory usage of our algorithm is shown in Figure 19 and Figure 20.



```
Filename: FakeAp.py

Line #    Mem usage    Increment   Line Contents
================================================
    11     28.1 MiB     28.1 MiB   @profile
    12                             def getAverage
    13                                 global ave
    14     28.1 MiB      0.0 MiB       capture =
    15     31.2 MiB      2.3 MiB       for packet
    16     31.2 MiB      0.0 MiB           averag
    17     31.2 MiB      0.0 MiB           print(
    18                                 import pdb
    19                                 packetSequ
```

Figure 18. Memory used by proposed algorithm.

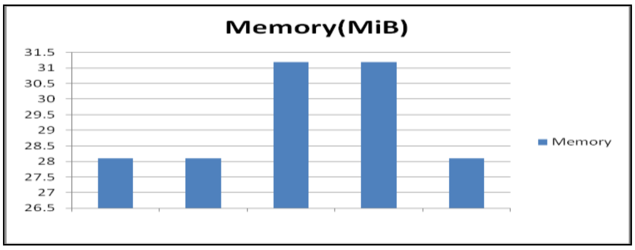


Figure 19. Average memory consumption by the proposed method.

VII. CONCLUSION

In this paper, we described a lightweight solution for detecting MITM Attack. The combination of two parameters i.e. sequence number and RSSI value are used to detect this attack. Taking these parameters alone can increase the false positives as these two parameters can be changed easily. Sequence number can be changed by the free tools available on the Internet and RSSI value depends upon a number of factors.

REFERENCES

1. Lanze, Fabian & Panchenko, Andriy & Ponce-Alcaide, Ignacio & Engel, Thomas. (2015). Hacker's toolbox: Detecting software-based 802.11 evil twin access points. 225-232. 10.1109/CCNC.2015.7157981.
2. T. R. Schmoyer, Y. X. Lim, and H. L. Owen, "Wireless intrusion detection and response: A case study using the classic man-in-the middle attack," in Proceedings of IEEE Wireless Communication and Networking Conference, 2004.
3. http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html
4. https://www.globalsign.com/en-in/blog/what-is-a-man-in-the-middle-attack/
5. Chen, Zhe, Shize Guo, Kangfeng Zheng, and Yixian Yang. "Modeling of man-in-the-middle attack in the wireless networks." In Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on, pp. 2255-2258. IEEE, 2007.
6. Zhang, Lizhuo, Weijia Jia, Sheng Wen, and Di Yao. "A man-in-the-middle attack on 3g-wlan interworking." In Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1, pp. 121-125. IEEE, 2010.
7. Nikbakhsh, Somayeh, Azizah Bt Abdul Manaf, Mazdak Zamani, and Maziar Janbeglou. "A novel approach for rogue access point detection on the client-side." In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pp. 684-687. IEEE, 2012.
8. de la Hoz, Enrique, Gary Cochrane, Jose Manuel Moreira-Lemus, Rafael Paez-Reyes, Ivan Marsa-Maestre, and Bernardo Alarcos. "Detecting and defeating advanced man-in-the-middle attacks against TLS." In 2014 6th International Conference On Cyber Conflict (CyCon 2014). 2014.
9. Dong, Ziqian Cecilia, Randolph Espejo, Yu Wan, and Wenjie Zhuang. "Detecting and Locating Man-in-the-Middle Attacks in Fixed Wireless Networks." CIT. Journal of Computing and Information Technology 23, no. 4 (2015): 283-293.
10. Han, Hao, et al. "A timing-based scheme for rogue AP detection." IEEE Transactions on parallel and distributed Systems 22.11 (2011): 1912-1925.
11. C. Yang, Y. Song and G. Gu, "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1638-1651, Oct. 2012.
12. Kim, Taebeom, et al. "Online detection of fake access points using received signal strengths." Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th. IEEE, 2012.
13. Gajbhiye, Yamini, and R. D. Daruwala. "RSS-based spoofing detection and localization algorithm in IEEE 802.11 wireless networks." Communication and Signal Processing (ICCSP), 2016 International Conference on. IEEE, 2016.
14. L. Rahman, "Detecting MITM Based on Challenge Request Protocol," 2015 IEEE 39th Annual Computer Software and Applications Conference, Taichung, 2015, pp. 625-626
15. Tang, Zhanyong, et al. "Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes." Mobile Information Systems 2017 (2017).
16. Ketkhaw, Apisak, and Sakchai Thipchaksurat. "Rogue access point detection mechanism considering sequence number of beacon frame for wireless local area networks." 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). IEEE, 2017.

17. http://www.sharetechnote.com/html/WLAN_FrameStructure.html
18. https://www.metageek.com/training/resources/understanding-rssi.htl

AUTHORS PROFILE

Rajinder Singh is an Assist. Professor in DCSA, PUSSGRC, Hoshiarpur, Punjab, India. He has more than fifteen years of experience of teaching post-graduate classes. His areas of interest are Wireless Network Security, Cyber Security, Artificial Intelligence and Android Security. He is currently pursuing His Ph.D. Degree from P.U. Chandigarh, India. His mail id is rajinderid@gmail.

Dr. Satish Kumar is Associate Professor in Department of Computer Science and Applications in Panjab University (PU), Chandigarh (India), currently posted at Panjab University SSG Regional Centre, Hoshiarpur, Punjab, India (a multi faculty prestigious campus of PU). He has more than fifteen years experience of teaching post-graduate classes. His areas of interest are Image Processing, Pattern Recognition, computer graphics and Artificial Intelligence. He can be reached at satishnotra@yahoo.co.in.