Wireless Security Threats

*Umair Jilani, **Muhammad Umar Khan, ***Adnan Afroz, **** Khawaja Masood Ahmed

***Abstract*—Wireless Communication Technologies has completely revolutionized the world. Wireless Communication Technologies provide ease to the users such as portability of the devices and mobile access to the internet. These portable wireless devices include PDAs, laptops, smart phones etc. offers some valuable features. These features include accessing the e-mails, SMS, MMS, calendars, addresses, phone numbers list and the internet. These entire devices store large amount of data and their wireless connection to network spectrum exhibit them as important source of computing. These devices are always vulnerable to attacks. Mobile devices are the new frontier for viruses, spam and other potential security threats. All these viruses, spam, Trojans and worms are out there in our vicinity to gain access to our personal data. This research aims to analyze the threats of viruses in the wireless communication systems and security including their role in the service outbreak, laying down the possible scenarios and also identifying possible remedies.**

***Index Terms*— Mobile Security, WEP, Authentication**

I. INTRODUCTION

Wireless communication is certainly the most rapidly developing area of telecommunication field. These days, wireless devices are gaining popularity and becoming the essentiality of every human being. Millions of users communicate and transfer their data wirelessly every instant. The main issue with the wireless technologies is securing the data. Many wireless protocols have been developed to provide security for the wireless networks. WEP (Wired Equivalent Privacy) is the first security solution designed for 802.11 LAN's. It was developed to provide the data confidentiality for the wireless networks up to the mark of traditional wired networks. The increase use in wireless network enables the standard wireless provides to make their network more secure. WiFi Alliance provides another security protocol WiFi Protected Access (WPA) for WLAN based on IEEE 802.11 specification. WiFi Protected Access (WPA) standard was designed to improve the security holes found in previous mechanisms. The security threats mean that hackers via different viruses and worms try to break into a secure network and gain access to protected data. They visualize an attacker doing exploit things by scan stealing, creating harmful exploits, this goes into account of targeted attackers. Dedicated attackers are the major concern for any organization, their main target is to break a network and go through the valuable information. Virus writers go after critical mass; they affect enormous number of people.

Wireless Communication systems are based on wireless transmission but besides certain advantages it has few disadvantages as compared to wired system. One of the major disadvantages is Bit Error Rate (BER). It is influenced by atmospheric noise, multi-path propagation, physical interference and potential interference caused from other systems. Interference within different bands is also a major problem as it didn't know the exact geographical ground location. To avoid this, licensing procedures were introduced in the form of the electromagnetic spectrum. Electromagnetic spectrum suggests the complete range of electromagnetic radiation. Electromagnetic spectrum consists of many parts called BANDS provided with different features.

Wireless Networks provide communication and transfer of data between two devices or more. There are many types of wireless networks and differ but mainly divided into three categories:

1. Wireless Wide Area Network (WWAN).
2. Wireless Local Area Network (WLANs).
3. Wireless Personal Ares Networks (WPAN).

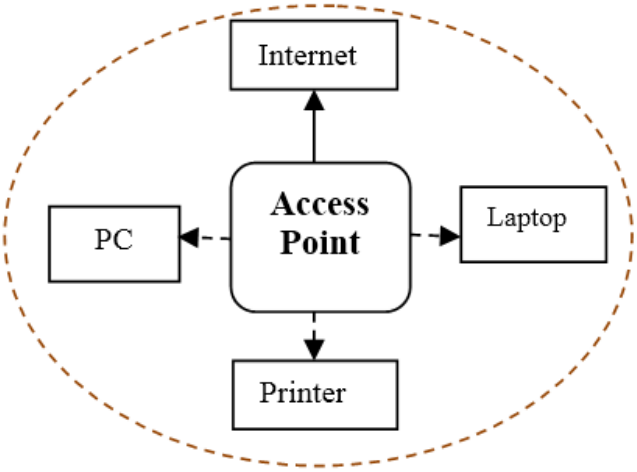

Fig. 1. Typical Radio Coverage

Governs by the Access Point, the wireless network offers us the radio waves instead of wires which ease the mobility of the device. Wireless Wide Area Networks (WWAN) has a broader coverage area than a WLAN. WWAN are the high power networks. The 3G and 4G mobile phone networks are examples of WWAN. Wireless Local Area Networks (WLAN) has a smaller coverage area. It is an IEEE 802.11 standard and provides WiFi access to the various corporate levels. Wireless Personal Area Network (WPAN) includes Bluetooth and Infra-Red technologies. They are low powered and unlicensed [3].

Department of Telecommunication Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan
*ujilani@gmail.com, **m_umar_k@hotmail.com, ***kmahmed@ssuet.edu.pk, ****adnaaf@hotmail.com

II. CELLULAR GENERATIONS

The first generation cellular systems launch in early eighties where systems are based on analog modulation techniques and have conventional cellular architecture. These systems work all around the world with transmission rate of about 2.4 kbps. There were certain drawbacks that where solved in future generations. They have no proper security mechanism as they used unsecured encryption techniques that largely results in identification spoofing. Late eighties saw the development of second generation cellular systems. At that time these designed systems were mainly used to transport voice data or traffic on the digital link. They were the first digitized systems including digital signal processing. They are circuit switched based network provide low data speed transfer. These basics are utilized in designing the digital systems and results in developing many standards specially GSM (Global System for Mobile), TDMA (Time Division Multiple Access, IS-54 / IS-136) in the US, Personal Digital Cellular (PDC) in Japan and another system in the US named CDMA (Code Division Multiple Access, IS-195) [2].

After 2G the race of 3G arrived but there is a 2.5G system between 2G and 3G systems. This is to improve capacity, high data rate up to 384 kbps and higher throughput for data service. The best feature of this generation is the optimizing channel for packet switched data to serve across internet [2]. As need of high data rate is fulfilled now the need of fast and secure multimedia communication is needed. That leads again the mobile supporter to start working systems beyond 3G system as generation revolution occurs once in decade.

III. ATTACKS ON WIRELESS NETWORKS

The security issue in the wireless systems has become quite essential due to the number of people dependent on these systems in their everyday life [2].

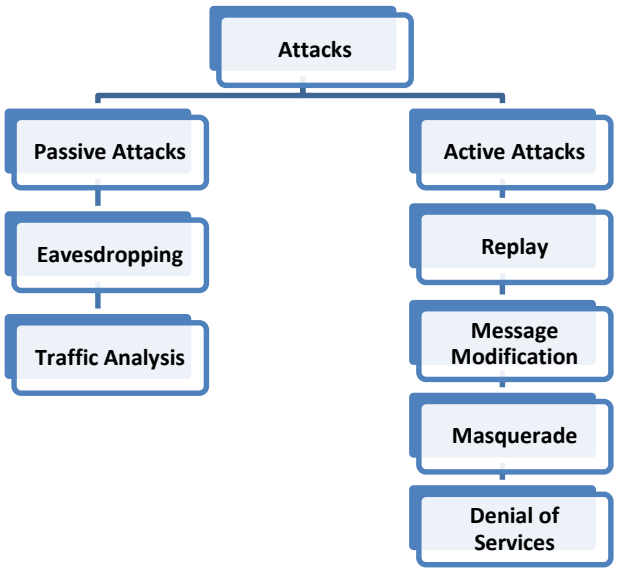

Fig. 2. Classification of Security Attacks

The attack on wireless system is characterized in two different types. Active attacks involve altering data or creating fraudulent streams. They can be sub classified as:

- *Masquerad:* Masquerade occurs when an entity pretends to be a different entity.
- *Reply:* In it data unit is captured by passive capture and also deals with retransmission.
- *Modification:* Modification involves the changing of messages for a certain portion of message that is changed or message that exhibits for unauthorized results.

Passive attacks are basically eavesdropping or spoofing on information in which the attacker tries to access the transmission that is being transmitted [2].

- *Release of message content:* This type of attack is on the transferred electronic mails or messages.
- *Traffic Analysis:* The attacker determines the location and identity of hosts along with the different transmission parameters as frequency and predicts the useful information of communicating users.

IV. WIRED EQUIVALENT PRIVACY WEP PROTOCOL

The name WEP is acronym of Wired Equivalent Privacy is modified form of previous security measures designed and its goal is to provide user a secure level of privacy as in wired Local Area Network. The purpose of this protocol designed to provide confidential and security. The two base stations utilizes a secret and unique key provided by WEP, these two stations might be affixed station as BSS and portable wireless enabled unit as laptop. In actual case or practical approach it utilizes a single network key between two network entities as in case of mobile station and access points. It has very delicate but very powerful management techniques to defend against the apparent attack on its communication.

There are many security algorithms that are being deployed by different protocols as in WEP case it utilizes encryption algorithm known as RC4 commonly known as stream cipher. It has operation mechanism of infinite pseudo-random key stream in which the existing key further expands. The receiving station is provided with copy of original key that is further used for generation confidential key. The original text is extract by XORing the cipher text with key stream [2].

The 802.11 standard has open system authentication and is the default form of this standard. It requires authentication from every user and this authentication based on embedded set of keys that are already provided between the wireless access points and wireless portable unit. Users only can access to the wireless service if it is authenticated by comparing the key provided by another user than the connection could not be

established. For transmission data is encrypted and an integrity check is made on packet to ensure safe transmission [2].

There are two specified methods by IEEE 802.11 for WEP. The first provides method enable windows with four keys that uses by station or access point to decrypt packets enciphered with these keys. The transmission is restricted to these manually entered four keys. Key Mapping is the second method where each company assigned MAC hardware address has unique separate keys that prevent the cryptographic attacks against other keys, but has a major disadvantage of manual configuration of each key on each device.

The shared authentication method is one in which the station that wishes to start or establish connection first sends a message that contains authentication requesting permission for shared key authentication.

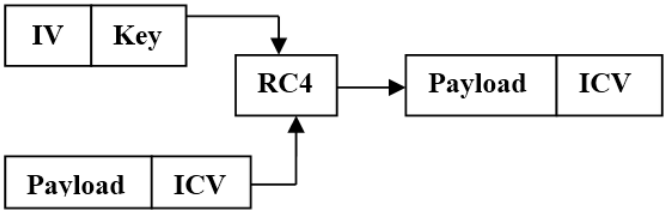

Fig. 3. WEP frame

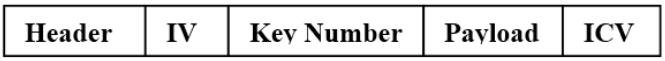

Fig. 4. Authenticated frame

Challenge text that is the authentication management frame send by responder is generated by Pseudo-random Number Generator (PRNG) that holds shared secret key and random vector. The content contained in this challenge text is copied by initiator to new management frame body; further this new management frame body is encrypted deploying the shared key with the initiating vector (IV). This new frame that includes Cyclic Redundancy Check (CRC) and Integrity Check Value (ICV) is received by responder that uses these CRC and ICV to decrypt the received frame; this text is then matches with the original text. If it matches then the switch role between initiator and responder and process is repeated.

A. *Encryption Computation Procedure For WEP*
Suppose a message that is to be transferred indicated by M.
SK=shared key.
IVS=initial vector,
PXT=plaintext.
CXT= cipher text.
RC4 is encryption algorithm [5].

1. The checksum and message concatenation P will be calculated as:

P = <M, CSK (M)>
2. Compute CXT=P RC4 (IVS, SK)
3. Finally, send IVS, CXT

In brief:

A →B: IVS, (<M,CS(M)> RC4(IVS, SK))

WEP DECRYPTION
1. Receive IVS and C
2. Compute CXT⊕RC4 (IVS, SK)
= (PXT⊕ RC4 (IVS, SK)) ⊕ RC4 (IVS, SK)
= P = <M ,ICS(M)>
1. Verify the integrity checksum ICS' (M) =ICS (M)
Now the secured message is received [5].

B. *Attacks Of WEP Privacy*
Consider CT1 and CT2 as cipher texts as CT1 representsPT1 (plaintext)

CT1 = PT1⊕RC4(IVS,SK)

CT2 = PT2⊕RC4(IVS,SK)

CT1 +CT2 =(PT1 RC4(IVS,SK)) (PT2 RC4(IVS,SK))

Now, you have PT2 since you have PT1.
Decipher all other cipher texts. WEP that contains checksum is true (linear) for the message function. Then,

I CS(x Y) =I CS(X) ⊕ICS(Y)

Suppose message received by the attacker <IVS, CT> as:

A goes to E: (IVS, CT)
E goes to B: (IVS, CT')

Let XE is a fabricate message with checksum ICS(X) then

((XE, ICS (XE)) ⊕CT =(X, ICS (XE)) ⊕ (((RC4 (IVS, SK)) ⊕<M, ICS (M)>)

=<XE, M>, (ICS (XE) ⊕ICS (M)) ⊕ (RC4(IVS,SK)

= (ICS (M ⊕ XE)),<M ⊕ X>⊕ (RC4 (IVS, SK)

=<M'>, (ICS (M')) ⊕ (RC4(IVS,SK)

C. *Flaws In The WEP Scheme*
The major flaws involve the RC4 algorithm and the initialization vector (IVS).Stream cipher operates on well-known algorithm of pseudo-random number key stream that deploy to expand a short key. This made it quiet applicable and strong threats against virus attacks. If an intruder try to change or flip single bit in cipher text a then the bit correspond in plain text will also be changed of flip. The two cipher text that have same shared key stream is intercept by eavesdropper then it is possible to XOR the two texts, this is useful for recovering the plain text against the statistical attacks. Once this text is recovered then it is helpful to recover the whole text. WEP stand as strong wall against all these two attacks. This method is

applied to ensure the correct transmission of packet and the intruders able to modify it. To make sure that the packet is transmitted correctly and it has being modified by any intruders during its transmission Integrity Check field in packet is used to verify it. Initialization Vector (IVS) is used against the possible ciphering of two texts and different RC4 is initialized for each Packet. IVS is also included in the packet. CRC-32 checksum is used in Integrity check fields error catching algorithm, checksum is a linear algorithm means it can calculate the transmitted bit differences between two CRCs included in messages. This can also be explain as reversing or flipping n numbers of bits in message block results to calculate the correct checksum by flipping the correct set of bits.RC4 decryption technique is used for flipping the bits has major flaw that didn't able to resist against the attacker to gain access to encrypted message and flip or change the bits along with the adjustment of checksum so that it look like that received message is delivered correctly.

As other packet structure Initialization Vector is 24-bit long and enables the use of same key that is used before. A busy access point, which constantly sends 1500 byte packets at 11Mbps, will exhaust the space of IVs after 1500*8/(11*10^6)*2^24 = 18000 seconds, or 5 hours [6]. This permits intruders or attackers to perform statistical attack for recovery of plain text by gaining access the two encrypted cipher keys (Encrypt with same key). This situation is further corrupted when mobile stations shared the same key increase the chances of IV collision.

V. MOBILE SECURITY ASPECTS

Different WiFi enable devices as Personal digital assistants, cell phones; wireless networks; satellite enabled telephone sets all are major threats to the different attackers. Mobile devices are the major hit by different malicious programs. Major concern in these sorts of attacks is digital images. The information added to the different image formats that are ideal weapon for the attackers.

A. Malware

Malware is basically used to define dangerous programs that cause severe damage to servers, computer, portable units as laptops, PDA. It is designed to damage or disrupt computers, applications, and networks. If allowed to enter a computer, malware can harm computer to a great deal and the information can be leak out. Malware divided into different harmful categories as Worms, Virus, Trojan, (PUP) and Hoaxes [2].

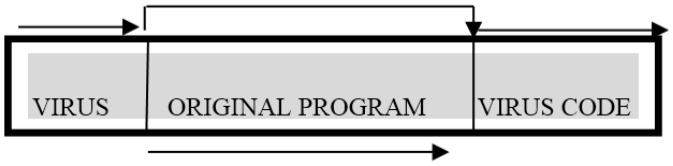

Fig. 5. How virus affects the original program

B. Virus

Cellular technology is also hit by this wireless threats and spread from mobile to mobile via different modes of message or file transfer as in case of Bluetooth operation, multimedia messages or various communication modes. Virus has a unique destructive code enter the mobile [9].

C. Worms

Another threatening designed program that spread itself once got entered in network. Wireless Attacks on mobile is with these worms can be harmful as data is being transferred. They don't have any central access points and spread on computer network at fast rate. Their purpose of design is to disturb the data transmission ability as they bear the self-replication property. The only difference in between worms and virus are that worms can spread it without any attachments where virus have to find some resources to attach itself and then perform hostile action. Worms utilizes the existing connection on network to spread itself. They are main threats to network speed as they consume bandwidth of network. Worms can also spread too many organizations that are working as a corporate network and perform malicious activities to the targeted source. They are becoming a major headache for user and network.

D. Trojans

Main resource to for any attacker to gain access to different file in our computer is Trojan virus. It does not replicate or propagate. Trojans are designed in such a manner that they destroy the system components of cell phone. They are basically handicap sort of virus as Trojan Horses largely effect the Symbian (Pocket PC like operating system similar to Microsoft) enabled cell phones and act in very destructive manner to the task designed in them but can't be able to make the replica of themselves. There may be several destructive functions attached to them that cause damage to mobile devices. Its main and most destructive sort of Trojan horse is that programs to ensure you to remove viruses from your device but instead of it put viruses on your device.

E. Hoaxes

Hoaxes are basically a warning of virus which can cause major disruption if nothing is done. They not only slow down traffic and clog up email servers, but they also cause people to panic. They make their way to computer when a person informs incoming of new viruses to another person. This is deliberately sent fake warnings instead of real viruses as they cause great use of network resources and also in terms company's money and time.

F. Potentially Unwanted Programs

These are basically the applications that look legitimate for some individuals but are undesired by many. These can be a key loggers, password crackers, spyware etc.

G. LTE Networks: Security Exposures

Wireless data, integrated services and multimedia applications are the major driving forces behind 4G LTE systems. These systems provide great flexibility and mobility to users but often they are exposed to security measures. The major security lack in 4G LTE system is that the encrypted data

in this case is terminated at Base station rather than end-user device. The security mechanism for 3G networks is seamless and authenticated and encrypted data is provided to end-users but in 4G LTE network only authenticated data is provided to end-users as indicated in Figure 5 and Figure 6. This encryption flaw will be overcome by certain countermeasure.

VI. THREAT ASSESSMENT

The passive attack to cellular technology has become major threat to millions of users as handheld devices become more complicated. Cellular networks equipped with internet that make vulnerable programs to gain easy access to these devices. Network service providers offer customer the always-on feature so that the mobile user to receive the messages at fastest rate. This internet facility being exploited by viruses and their replication property affects the wireless arena much more than before.

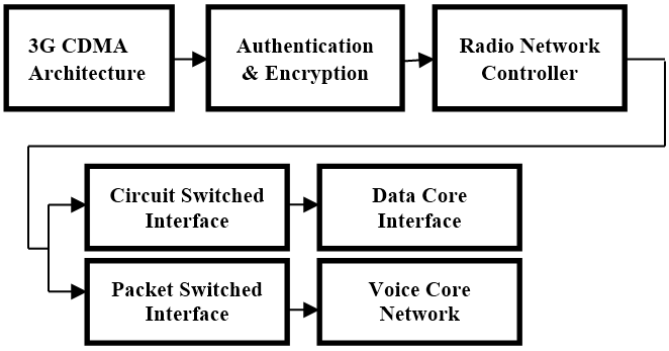

Fig. 6. Encryption in 3G Networks

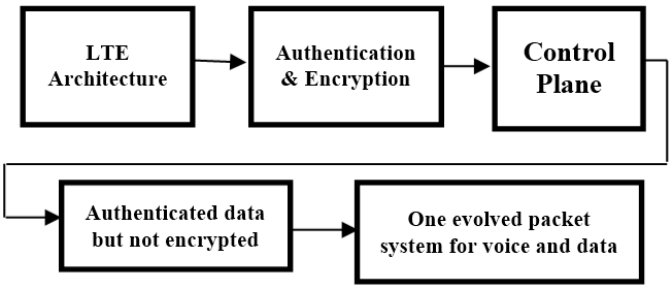

Fig. 7. Encryption in 4G LTE Networks

VII. COUNTERMEASURES

The preventive measures are being adopted against the security threats and countermeasures are taken to provide protection to the mobile devices from these attacks. These countermeasures include essential preventive measures that should be adopted in making calls, accepting files from other hand-handle devices, receiving image or executable files, installation of freeware or shareware software.

A. Authentication

The process of reorganization and verification to ensure the validity of user or devices requesting for connection is carried through Identification and Authentication (I&A) process. Multiple authentication procedures by using passwords or pattern matching are available for this purpose. At primary level the strong emphasis by vendors should be implemented on user education regarding this purpose. There certain tools are available to cracked password and the network administrator and user should audit their password on regular basis. Hand handle devices are also equipped with the powerful Biometric authentication technology.

They use user fingerprints as the authentication process for hand handle devices via USB port or serial connection can be used to lock the application of individual user or to lock the whole cell device or connection to remote places and access the database over existing network. Tamperproof SIMS, provided with unique code for identifying the user information, contain private key that is used to authenticate user on the network. This leads to the secure connection as the intruders must have knowledge about these keys so that he can gain access to the network. There are certain measures for handheld devices as flash ID, device ID and Electronic Serial Number (ESN) o authenticate them on any available network as two-factor authentication.

B. Public Key Infrastructure (PKI)

Different hand-handled devices are equipped with the support for PKI as it proves to be one of the best tool for the ensuring the security measures. A PKI uses an asymmetric encryption method, commonly known as the public/private key method, for encrypting and ensuring the integrity of documents and messages [10]. Digital certificates are used by certificate authorities to provide a proper authentication for users and organizations on internet. Many applications such as Electronic Email and Web browsers are already embedded with PKI features so they verified for valid signatures and certificates. The PKI provided with encryption algorithms, certain assignment of keys to user along with acquired levels of security. Many organizations implement PKI by themselves so as to prevent the sensitive information of users. Number of threats being encountered by PKI in public networks; additionally include hardware and software expenditures that are performed during the preventive measures against the security requirements of any agency.

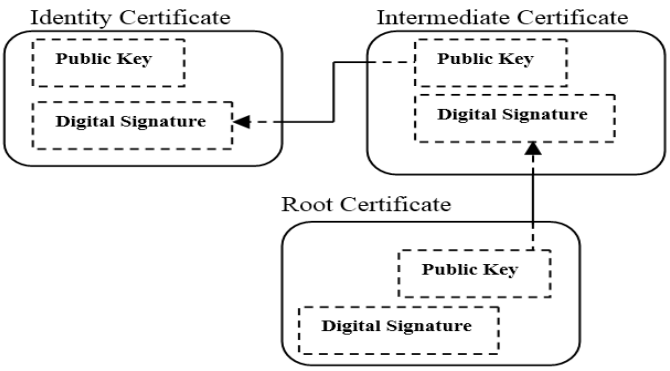

Fig. 8. HTTPS Example

The primary example of PKI is Hyper Text Protocol Secure (HTTPS) that is the combination of HTP and SSL to ensure user for better and secure communication on web server.

C. Solutions for Wireless Gateway

The scanning for viruses is not only the issue but the proper protection against these attacks as they disguised in many forms. Inter-scan use the technology that is a group of certain rules along with the Script Trap that maintain the virus analysis and any suspicious activity create by them. For instance if the code has designed in such a way that it automatically dial number as 911 then it locks the code as it was against the desire of user. Electronic Manger (e-Manager) is provided with the rules-sets that contain the wireless spamming tools as Timofonica Trojan and the flaws as buffer overflow.

D. Preventive Measures for WLANs

1) *Controlling The Broadcast Area:* The signal strength and its directions are two prime factors that are adjusted by Access Points (AP). The AP are marked and placed at same distance from walls, then signal strength is altered and exterior connections are hard to establish. So it is desired to place AP at points where there are less chances of signal distortion.

2) *Locking Of APs:* It is desired and essential for every person that they should change the default AP and administrator password so that they prevent themselves from the tempting target of wireless attackers.

3) *Utilize 128-Bit WEP:* WEP protocol stand still wall against skilled hacker that use Linux Freeware and make it difficult for attackers to gain access to wireless network.

4) *Proper Use to SSID:* The SSIDs should be changed accordingly and it should be keep concerned that the SSID should not be as simple as easy to use. The proper arrangement should be made for secure SSID.

5) *Limit The Number Of User Addresses:* DHCP addresses that are assigned by network should be limited depending on the number of users. This provides the list of unauthorized users as there are limited numbers of channels allocated.

E. Preventive Measures for 4GLTE Networks

In contrast to 3G networks where RNC is responsible for security buffer between core and access network the LTE networks are secured by S1-Flex feature allowing different subscriber to be attached to any node in network. In order to avoid any user to gain access to clear text stream they can potentially trigger an outage or can access directly to operator's services as Voice over LTE (VoLTE) ensure to change.

VIII. CONCLUSION

The above research shows a better approach to overcome the threats of viruses by knowing their presence in various wireless modes. It is being observed that presently there is no such virus that can be automatically installed itself in any system rather than it needs a social engineering technique to spread out in the system. It is also recommended to always install applications including software, games, music etc. from a trusted resource. Always keep the Bluetooth devices in undiscoverable mode so that an intruder cannot break into the system easily. Human negligence can also become a cause of virus installation, therefore always use update antivirus software that can scan the system periodically and have the tendency to block it well before penetrating into the system.

REFERENCES

[1] Schirmer, Mark. "A Year of CAN-SPAM, a Year of More Spam." *Foresight* 43 (2005).

[2] Ahmad Naseer, "Security Issues in Wireless Systems", M.S. Thesis, School of Computing, BTH, July, 2009.

[3] Rahul Seth and Ahmad Alshareef (2003, December 07), Photonic Center Wireless Network. Available: http://nislab.bu.edu/nislab/education/sc441/one/intro.htm

[4] Nicopolitidis, P., M. S. Obaidat, G. I. Papadimitriou, and A. S. Pomportsis. "Wireless Communications Principles and Fundamentals." *Wireless Networks* (2009): 25-94.

[5] Lucaskauffan (2013, August 28), Wifi Security. Available:http://security.blogoverflow.com/2013/08/wifi-security-history-of-insecurities-in-wep-wpa-and-wpa2/

[6] Scarfone Karen, Paul Hoffman, and Murugiah Souppaya. "Guide to enterprise telework and remote access security", *NIST Special Publication 800 (2009):46.*

[7] Borisov, Nikita, Ian Golderg, and David Wagner. "Intercepting mobile communication: the insecurity of 802.11", *In Proceedings of the 7th annual international conference on mobile computing and networking*, pp. 180-189, ACM, 2001.

[8] Mezzadra, Sandro, and Brett Neilson. *Border as Method, or, the Multiplication of Labor.* Duke University Press, 2013.

[9] Kuhn, D. Richard, Vincent C. Hu, W. Timothy Polk, and Shu-Jen Chang. *Introduction to public key technology and the federal PKI infrastructure*. National Inst of Standards and Technology Gaithersburg MD, 2001.

[10] Guideline on Wireless Security (2012, March), Issue No. 3. Available:http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20on%20Wireless%20Security.pdf