# Security Issues In Wireless Networks

V. Karthick Reddy [1] Ch. Ravi Chandra Gupta [2] Assoc.Prof. T. Ravi

*B.Tech, K.L.University* *B.Tech, K.L.University* *Assoc.Prof, K.L.University*

## Abstract

*Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections-without requiring network or peripheral cabling. Wireless technologies use radio frequency transmission as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. A brief overview of wireless networks, devices, standards and security issues is presented in this section.*

*Security is an essential component of a mobile deployment, but must be carefully considered so the organization reduces its risks while also reaping the rewards. Mobile workers do not generally adopt technologies or adhere to security practices that impede their productivity or hinder them from doing their "real job." Security must be implemented without substantially degrading worker productivity and overall usability, or the mobility project will likely fail to meet its business objectives.*

***Index Terms***- OSA, GSM, Algorithm, DOS

## 1. Introduction

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks. Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range. Wireless Wide Area Wireless (WWAN), WLANs and Wireless Personal Area Networks (WPAN). Global system for Mobile Communication (GSM), and Mobitex. WLAN representing wireless local area networks includes 802.11, Hyper LAN, and several others. WPAN represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are "tether less" they receive and transmit information using electromagnetic waves. Wireless technologies use wavelengths ranging from the radio frequency band up to and above the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communication frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy into the IR and then the visible spectrum. This document focuses on WLAN and WPAN technologies

## 2. Security Threats

All computer systems and communications channels face security threats that can compromise systems, the services provided by the systems, and the data stored on or transmitted between systems. The most common threats are as follows:

- Denial-of-service
- Interception
- Manipulation
- Masquerading
- Repudiation

### 2.1. Denial-of-service (DOS)

It occurs when an adversary causes a system or a network to become unavailable to legitimate users

and also causes services to be interrupted or delayed. Consequences can range from a measurable reduction in performance to the complete failure of the system. There is that can be done to keep a serious adversary from mounting a denial of service attack.

### 2.2. Interception

It has more than one meaning. A user's identity can be intercepted leading to a later instance of masquerading as a legitimate user or a data stream can be intercepted and decrypted for the purpose of disclosing otherwise private information. In either case the adversary is attacking the confidentiality or privacy of the information that would be intercepted. An example would be eaves dropping and capturing the wireless interchanges between a wireless device and the network access point. Since wireless systems use the radio band for transmission, all transmissions can be readily intercepted. Therefore, some form a strong authentication and encryption is necessary in order to keep the contents of intercepted signals from being disclosed.

### 2.3. Manipulation

It means that data has been inserted, deleted, or otherwise modified on a system or during transmission. This is an attack on the integrity of either the data transmission or on the data stored on system. An example would be the insertion of a Trojan program or virus on a user device or into the network. Protection of access to the network and its attached systems is one means of avoiding manipulation

### 2.4. Masquerading

It refers to the act of an adversary posing as a legitimate user in order to gain access to a wireless network or a system served by the network. For example a user with inappropriate access to a valid network authenticator could access the network and perform unacceptable functions strong authentication is required to avoid masquerade attacks.

### 2.5. Repudiation

It is when a user denies having performed an action on the network. Users might deny having sent a particular message or deny accessing the network and performing some action. Strong authentication of users, integrity assurance methods, and digital signature can minimize the possibility of repudiation.

## 3. Security Services and Vulnerability

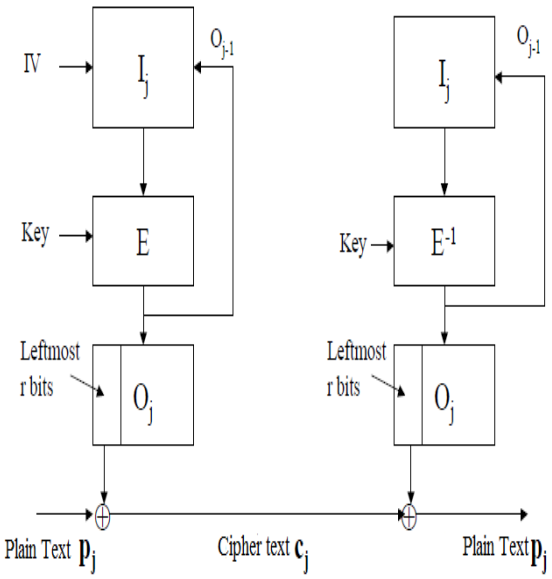
Two security services are specified in IEEE 802.11, the authentication service and the privacy service. The privacy service is provided by the wired equivalent privacy (WEP) algorithm. The authentication service provides two basic levels of security. The first open system authentication (OSA) is mandatory, but provides essentially no security. The second is shared-key authentication that provides the highest level of security available and uses the WEP algorithm.OSA exchanges messages between a station and the wireless access point. Any station that can successfully send and receive complaint messages is permitted to associate with and enter the network Shared key authentication specifies a number of requirements intended to defeat or mitigate some of the threats mentioned earlier. Particular attention was paid to

- Authenticating users over an encrypted channel
- Defeating an adversary's ability to eavesdrop on wireless transmissions in order to preserve confidentiality by encrypting the channel traffic and
- Providing integrity assurance that a message was not modified in transit

## 4. Wired Equivalence Privacy (WEP)

The WEP is based on the use of RC4 is a stream cipher developed in 1987 by Ron Rivest at MIT for RSA data security. The algorithm was kept secret for the first 7 years, but was anonymously posted to the cypherpunks mailing list in 1994 and it quickly spread to news and ftb sites around the world. Although it is now public, analysis indicates that RC4 is still a strong algorithm and is immune to linear and differential cryptanalysis, is very non-linear, and does

not have short cycles. RC4 is used in many commercial products. RC4 as specified in the standard operates in output feedback (OFB) mode.




The RC4 algorithm has three inputs an initializing vector IV, the random key, and the plaintext. The 1V vector is input to E, the RC4 encryption algorithm along with the key. The algorithm generates a key stream output from E that is sent to the output box O. the output box O shifts the key stream out, a byte at a time and each bite is combined with the plaintext p under the exclusive OR function. The output of E is also fed back to the 1 stage which causes the key stream to vary as a function of 1V and the key.

That is:

Given: The plaintext pj and RC4(IV, Key)

Form: cj = pj □□RC4(IV, Key)

Encryption is shown on the left and decryption on the right side of figure 1.

Since IV must be known to the transmitter and receiver, it is sent to the receiver as an unencrypted part of the cipher text stream. The logic function to insert IV into the cipher text stream and recover it from the stream for input to the I function at the receiving end are not shown, but are straight forward functions. IV does not have to be secret since RC4's strength is derived from the algorithm and key, not IV. However, the integrity of IV needs to be assured or decryption will not function properly.

The RC4 algorithm supports variable length keys. The two lengths most commonly used for wireless applications are 40 bits for export controlled systems and 128 bit encryption, the effective key length is 104 bits One of the primary requirements of stream ciphers in general and RC4 as well is that the implementation must ensure that key stream is never used twice to encrypt a data stream.

### 4.1. Key management

The standard does not specify how keys are managed or distributed. It does provide for an externally populated globally shared array of 4 keys. In addition, it allows for an additional array that associates a unique key with each user station. Most of the existing implementations utilize the globally shared array of secret keys to encrypt the link transmission between users and the wireless network access point. A single key can be used, it is made known to all users and the access point. If more than one key is used, it is known to all users in the group associated with the key. Some access points allow for two channels such that the keys for each channel can be different. Devices assigned to one channel still share the secret key with other users assigned to that channel and the access point.

### 4.2. Integrity assurance

The input Pj string is composed of the original message M with a CRC32 checksum of the message appended to the end of the message. The purpose of the checksum is to provide the integrity service that is described later.

Therefore:

Given PM a plaintext message string, compute the checksum of PM=c(PM) and concatenate the two parts to produce the plaintext P=PM, c(PM).

At the receiver the cipher text is decrypted, then the CRC32 bit string is calculated on the original plaintext input string and compared to the CRC32

received. If the CRCs match then the original message is accepted as valid. This is a well-know method for not ensure cryptographic integrity Vulnerabilities and weaknesses

### 4.3. Authentication

Prior to sending data and an access point must authentication and establish. An association is a binding between the station and the access point. The process for this consists of three states

- Unauthenticated and unassociated
- Authentication and unassociated
- Authentication and associated

Once successfully authenticated and associated stations can exchange data with the access point. As indicated earlier, two authentication methods are supported. Open System authentication and Shared key Authentication

### 4.4. Open System Authentication

Open System Authentication (OSA) is a mandatory standard requirement and is the default authentication method. In OSA two management frames are exchanged between the station and the access point (AP). The first frame is sent from the station to the AP and includes the station Media Access Control (MAC) address and an identifier indicating it is an authentication request. The AP responds with a second frame that includes a status field indicating authentication success or failure. The station is now authenticated and unassociated. Two more frames are passed to establish and association. Most wireless vendors have implemented a wireless access control mechanism as part of the association process that is based on examining the station MAC address and blocking unwanted stations from associating. Support for this requires that a list of authorized MAC address be loaded on AP.

This approach has several problems. Identifying and loading MAC then keeping them current is manually intensive. An adversary seeking access to the network could monitor the network and capture legitimate MAC address and associated with the AP ganging access to the network. This also has the potential to create network problems if two stations with the same addresses attempt to use the network at the same time.

In any case OSA is not recommended. tn the default case requesting station can be authenticated and associated, in cases where the manufacturer of the network equipment support MAC address access control. The addresses can be readily spoofed and allow inappropriate access as well as potentially causing network problems

### 4.5. Shared Key Authentication

Shared key authentication uses the optional along with a challenge response system to mutually authenticate a station and an AP. Authentication consists of the exchange of 4 messages for station authentication and 4 more for AP authentication. APs send “beacon” messages to announce their presence. A station wishing to enter the network finds a beacon message and then initiates authentication with the AP whose address appears in the beacon message. The exchange is shown in figure 2


The initiating station sends a management frame (sequence # 1) to the AP requesting authentication. The frame is sent in the clear. The responding AP sends sequence #2 which contains an authentication challenge in the message body. The challenge is 128 octets length.

The AP challenge is generated by combining a pseudo random number with the shared secret key and a random initializing vector (IV) and sent as a clear text message The station receives the message

extracts the challenge and copies it to a new management frame. This frame is encrypted under the WEP algorithm using the shared key and a 'new' IV and sent to the AP. The IV used by the station is also sent to the AP in the clear so the AP knows what IV to use with the secret key to decrypt the frame.

The AP receives the frame, decrypts the contents, and checks the validity of the CRC 32 check sum, and tests the challenge to see if it matches the original challenge sent to the station. If the CRC 32 check is invalid, the frame is dropped. If the CRC-32 is valid, the challenge is tested. On a match the station is successfully authenticated. The process is repeated to authenticate the AP to the station. The protocol for exchanging authentication messages can be exploited to allow unauthorized stations to enter the network. In this exploit, an unauthorized station monitors the exchange just described and captures the second and third exchanges. The second frame contains the unencrypted challenge and the third frame contains the encrypted challenge. The unauthorized station has the following information.

- The plaintext of the original frame including the random challenge
- The encrypted frame containing the challenge, and
- The IV used to encrypt the challenge.

The exclusive OR of the plaintext P and the cipher text C will produce the key stream used to encrypt the challenge response frame. The unauthorized station will not have the shared secret key, but given the key stream, the unauthorized station can enter the network. That is, the unauthorized station now requests authentication to the network. In response, the AP sends a new challenge frame. This challenge frame will have a different content and a different CRC-32 check sum. The invader computes a valid CRC-32 check sum encrypts the challenge with the key stream acquired earlier, appends the IV used and sends the frame

While this authenticates the unauthorized user, the network cannot be used unless the shared key is also broken since only having access to a single valid key stream is not sufficient for further communication using the WEP algorithm. Methods for acquiring the secret key are described later.

## 5. RC4 Encryption

There is nothing inherently wrong with RC4 unfortunately and WEP is not a secure implementation of RC4 and violates several other cryptographic design and implementation principles [WALK00]

### 5.1. Interception

In some cases attacks depend on the ability of an adversary to intercept wireless traffic. Fundamentally, we know that any traffic transmitted by ratio signal is subject to interception since it is a radio frequency broadcast. The IEEE 802.11 standard specifies three possible physical layers. Infrared (IR). Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS) and broadcasts in three frequency bands, 900 MHz, 2.4GHz. and 5 GHz. Most products currently being fielded use DSSS and the 2.4 GHz band . interception is an easy matter even for service for relatively unskilled adversaries. That is because any commercial wireless device designed for service in the appropriate band of frequencies is readily capable of receiving all signals. It is then a relatively easy matter to modify device and flash memory to promiscuously monitor all traffic. Consequently, it should be assumed that an adversary has access to intercepted signals.

### 5.2. Key stream reuse

We have described on the basic operation of RC4 as illustrated in Figure 1. One of the well known attributes of stream ciphers operating in output feedback mode on that encrypting two messages under the same IV and key that it can reveal information about both messages to a cryptanalyst. Consider the encryption of two plaintexts, P1 and P2 as follows:
C1 = P1 Å RC4 (IV, K), and
C2 = P2 Å RC4(IV, K), then
C1 Å C2 = (P1 Å RC4 (IV, K)) Å (P2 Å RC4(IV, K))
If the same IV and Key are used, then
C1 Å C2 = P1 Å P2

That is, the Exclusive OR of the two cipher texts will produce the Exclusive OR of the two plaintexts. Thus, if the plaintext of one message is known, the plaintext of the other message is revealed. One way to achieve this would be for an attacker to send a known plaintext message to a wireless device and then intercept the encrypted message associated with the plaintext. While this raises a number of difficulties, it is a feasible attack.

The traffic must be intercepted and an adversary must find an instance of the same key and same IV being associated with one, or more, other messages (i.e., other than the one the adversary injected) on the network. Since the shared key is used by multiple stations the requirement for the use of the same key is satisfied. Consequently, the adversary must find messages using the same IV.

Reading the IV is trivial. The IV is transmitted in the clear (i.e., unencrypted) with every packet. Recovering an IV with the same value depends on how well IVs are initialized, how well they are constructed (e.g., the size of the IV space (length in bits)), and how often they are re-used in a typical network.

The standard recommends, but does not require, changing the IV for every frame transmitted. It provides no guidance on selecting or initializing the IV. The work at UC Berkeley indicates that some PCMCIA cards reset the IV to zero when initialized and then increment the IV by one for each packet transmitted [BORI01]. This is a relatively predictable pattern and it can be expected that a relatively higher proportion of low valued IV's would appear on the network than would be expected in the IV's were randomly initialized.

In order to execute this attack the adversary would have to capture packets and compare IV values searching for collisions. A collision would allow analysis of a single packet. If the plaintext of one packet is known and is carefully selected, then the plaintext of the other packet would be revealed.

It is a relatively simple matter to get a known plaintext injected into the network by injecting a message from outside the network, but addressed to a mobile user on the network. Monitoring transmissions is somewhat more difficult, but can be done by operating a mobile device in promiscuous mode as discussed earlier. Once the key is revealed all transmissions using that key and IV are compromised.

The process is simplified to a great extent if the IV is not changed every packet. The standard recommends, but does not require, the IV to be changed every packet.

### 5.3. Integrity assurance:

The standard specifies an integrity algorithm the operates based on the original plaintext message to produce an integrity check value (ICV). The original plaintext is concatenated with the IVC to form the plaintext to be encrypted. the IVC method is specified in standard is CRC-32.the IVC is a 32-bit field called the FCS field and it is defined as the lat 4 octet in the MAC frame. Since the CRC-32 function is a linear function that are used only addition and multiplication, it is possible to change one, or more, bit in the original plaintext and be able to predicted the bit to change in the CRC-32 checksum such that the check sum remains valid when it i received. Integrity methods that are cryptographically secure such as hah algorithm are non-linear functions that are not readily attacked. what this means is that it is possible to modify legitimate message and insert them in the data stream without detection. This is probably not a concern for that messages presented by the application for transmission. However, the checksum is highly performed over the entire MAC packet and that includes higher-level protocol routing to all address and port fields. If an adversary turns his or her attention to modification of the IP destination field, it is possible to re-direct traffic to an unintended destination under the control of the adversary. In addition, the capability to forge valid CRC-32 checksums is required to carry out the authentication attack described earlier.

### 5.4. Existing Products

In order to field a compatible implementation of the standard, vendors must implement to all mandatory features of the standard. In some cases, like the use of CRC-32 for that integrity, the standard is weak by design and needs to be changed. Until that happens, products will continue to be implemented with known weaknesses. In other cases, stronger security measures are possible without violating the standard. Key

management, for example, is a function that is external to the standard and can be implemented to all products as a product developer sees fit. While this creates the issue of that interoperability limiting the selection of products for the organization that desires to be highly stronger protection most vendors do offer options that strengthen security. The point to be made is that specific products must meet the standard, but may be extended in various ways to improve security. Products are changing rapidly and the prospective implementer should be diligent about getting the most recent vendor information.

There continues to be on-going development of the standard and a part of that development is stronger security measures. The chairman of the IEEE 802 committee has publicly responded to the threat and vulnerabilities raised by the U. C. Berkeley team. Some of his more important comments are paraphrased a follow [KELL01]:

1. WEP was never intended to provide more protection than a physically protected LAN environment. Since most LAN's are physically protected from external access, WEP was designed for equivalency protection from casual eavesdropping. WEP was never intended to be a complete security solution. Like wired LANs, a wireless network needs to be augmented with additional security mechanisms (e.g., end-to-end encryptions, virtual private networks, etc.), as appropriate to that requirements of the user organization.
2. The active attacks are not easy to mount. They are conceivable given enough time and resources, but may not yield enough value to an adversary to be worthwhile.

## 6. Conclusion

During the last decade we have witnessed a tremendous growth within the wireless communication industry. Customers want speed and improved performance, but only if it comes with reliable services. This requires fundamental rethinking of the traditional pure performance model that ignores failure, repair or recovery but mainly concentrates on resource contention. To reflect a real-world system in realistic way, availability, capacity and performance issues of a network should be considered in an integrated way. In this paper, we have presented the CTMC, MRM and SRN models for per formability study of a variety of wireless systems. By solving the two-level models, we can compute per formability measures, such as call blocking probability and handoff call dropping probability, for wireless systems and wireless cellular systems with handoff, base repeaters, and control channels.

.

## 7. References

[1]. [ARBA01] Arbaugh, William A., N. Shanker, and Y.C. J. Wan, "Your 802.11 Wireless Network Has No Clothes." URL; http://www.cs.umd.edu/~waa/wireless.pdf (14 Nov.01). [2].[BORI01] Borisov, N, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: TheInsecurityof802.11."URL;http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf)

[3]. [BORI01-3] Borisov, N, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11."URL;http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.Pg.3.(15Nov.01).

[4].Borisov, N., I. Goldberg, and D. Wagner, "Security of thWEPAlgorithm."URL:http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html(14Nov.01)

AUTHORS

**V.Karthick Reddy** was born in 1992 at kadapa, Andhra Pradesh. He is pursuing his B.Tech in KLUniversity in Electronics and Communications. His interested areas are wireless communication, Data communication. (email:vkarthickreddy@gmail.com, ph.no:9492066228).

**Ch.Ravi Chandra Gupta** was born in 1992 at Guntur, Andhra Pradesh. He is pursuing his B. Tech in KLUniversity in Electronics and Communications. His interested areas are wireless communication, Data communication.(email:12ravichandra34@gmail.com)

**T.Ravi** did his B.Tech at KSRMCE Kadapa and later he did his M.E at Karunya University and M.Tech in JNTU Kakinada. He worked as HOD in Universal College of Engg. and Tech. Guntur. And presently he is working as Assoc. prof in KLUniversity. His interested are wireless communication and image processing.