ENHANCING MESSAGE PRIVACY IN WEP

by

DARSHAN SHRINATH PURANDARE
B.S. Computer Science REC Bhopal, India 2001

A thesis submitted in partial fulfillment of the requirements
for the degree of Master of Science
in the Department of Computer Science
in the College of Engineering
at the University of Central Florida
Orlando, Florida

Spring Term
2005

Major Professor: Ratan Kumar Guha

ABSTRACT

The 802.11 standard defines the Wired Equivalent Privacy (WEP) and encapsulation of data frames. It is intended to provide data privacy to the level of a wired network. WEP suffered threat of attacks from hackers owing to certain security shortcomings in the WEP protocol. Lately, many new protocols like WiFi Protected Access (WPA), WPA2, Robust Secure Network (RSN) and 802.11i have come into being, yet their implementation is fairly limited. Despite its shortcomings one cannot undermine the importance of WEP as it still remains the most widely used system and we chose to address certain security issues and propose some modifications to make it more secure. In this thesis we have proposed a modification to the existing WEP protocol to make it more secure. We achieve Message Privacy by ensuring that the encryption is not breached. The idea is to update the shared secret key frequently based on factors like network traffic and number of transmitted frames. We also develop an Initialization Vector (IV) avoidance algorithm that eliminates IV collision problem. The idea is to partition the IV bits among different wireless hosts in a predetermined manner unique to every node. We can use all possible 2^{24} different IVs without making them predictable for an attacker. Our proposed algorithm eliminates the IV collision ensuring Message Privacy that further strengthens security of the existing WEP. We show that frequent rekeying thwarts all kinds of cryptanalytic attacks on the WEP.

To My Parents

ACKNOWLEDGMENTS

I take this opportunity to express my heartfelt gratitude to all those who have directly or indirectly contributed to the success of my work.

My most sincere thanks to Dr.Ratan Guha who has been a great source of help and inspiration. He guided me all throughout and took painstaking efforts towards the completion of the work. Special thanks to Dr. Mostafa Bassiouni and Dr. Johan Lee for their guidance and support.

My work was partially supported by NSF under grant EIA 0086251 and ARO under grant DAAD19-01-1-0502. I will always be indebted to them.

Gautami and Oguz deserve a special mention for being my best pals and mentors. My childhood friend Abhishek Srivastava even though didn't do anything except wasting my time also deserves a special mention.

Last but not the least I thank everyone involved who made this thesis an experience I will forever cherish.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS/ABBREVIATIONS

AP	Access Point
BSS	Basic Service Set
CRC	Cyclic Redundancy Check
DSS	Distribution System Services
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IV	Initialization Vector
KSA	Key-Scheduling Algorithm
LAN	Large Area Network
LLC	Logical Link Control
MAC	Media Access Layer
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
OCB	Offset Codebook Mode
RC4	Rivest Cipher or Ron's Code
RSN	Robust Secure Network
SS	System Services
WAN	Wide Area Network
WEP	Wires Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi- Fi Protected Access

CHAPTER ONE: INTRODUCTION

Last few years have seen the advent of wireless technologies and IEEE 802.11 standards for wireless LAN [3] is one among them. The 802.11 standard defines the Wired Equivalent Privacy (WEP) and encapsulation of data frames. It is intended to provide data privacy to the level of a wired network. These standards have been accepted by the industry; related hardware is available and is in widespread use. Wireless cards for laptops, wireless routers (access points) are in use everywhere ranging from large scale infrastructures to home networks. However, with this added convenience and luxury, it suffered threat of attacks from hackers owing to certain security shortcomings in the WEP protocol. Lately, many new protocols like WiFi Protected Access (WPA), WPA2, Robust Secure Network (RSN) and 802.11i have come into being, yet their implementation is fairly limited. Despite its shortcomings one cannot undermine the importance of WEP and we chose to address certain security issues and propose some modifications to make it more secure. Over the years many type of attacks have been identified on WEP.

WEP failed to achieve its goals in almost all the areas including authentication, access control, replay prevention, message modification detection, message privacy and key protection [6]. Serious security flaws like presence of relatively short Initialization vectors (IVs) [4], keys that remain static, subtle vulnerability in RC4 algorithm's [2] usage in the WEP has made it relatively weak. We have focused mainly on the issue of message privacy because this is the most important security mechanism in the WEP. An attacker cannot accomplish much if the encryption method stays strong and unbroken. However, if an intruder gets the keys then he is into the system as a legitimate user and can perform all the malicious activities without getting

noticed. Message Privacy thus becomes the most critical issue among all the security mechanisms of WEP. If we can ensure that the transmitted data in the air cannot be decrypted by the attacker in its meaningful time we achieve the notion of Message Privacy. We propose a modification to the existing WEP protocol and also develop an IV avoidance algorithm to make WEP more secure and achieve Message Privacy. Chapter 2 is devoted to the description of the WEP protocol. Chapter 3 looks at the previous work done in the research community to improve WEP. Chapter 4 identifies the security flaws in the WEP protocol. Chapter 5 talks about our proposed idea to modify the WEP protocol. It includes an IV avoidance algorithm and an access point key management system. We analyze and enumerate the features of our protocol in Chapter 6. Subsequently, we have our conclusion and references.

CHAPTER TWO: RELATED WORK

2.1 IEEE 802.11 Standards

IEEE 802.11 or Wi-Fi denotes a set of Wireless LAN standards developed by working group 11 of the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The term is also used to refer to the original 802.11, which is now sometimes called "802.11 legacy".

A wireless LAN (WLAN) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure. The 802.11 specification as a standard for wireless LANs was ratified by the IEEE in the year 1997. This version of 802.11 provides for 1 Mbps and 2 Mbps data rates and a set of fundamental signaling methods and other services. Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels of the ISO model, the physical layer and link layer shown in Figure 1. Any LAN application, network operating system, protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

The 802.11 standard addresses:

- Functions required for an 802.11 compliant device to operate either in a peer-to-peer fashion or integrated with an existing wired LAN

- Operation of the 802.11 device within possibly overlapping 802.11 wireless LANs and the mobility of this device between multiple wireless LANs
- MAC level access control and data delivery services to allow high layers of the 802.11 network
- Several physical layer signaling techniques and interfaces
- Privacy and security of user data being transferred over the wireless media

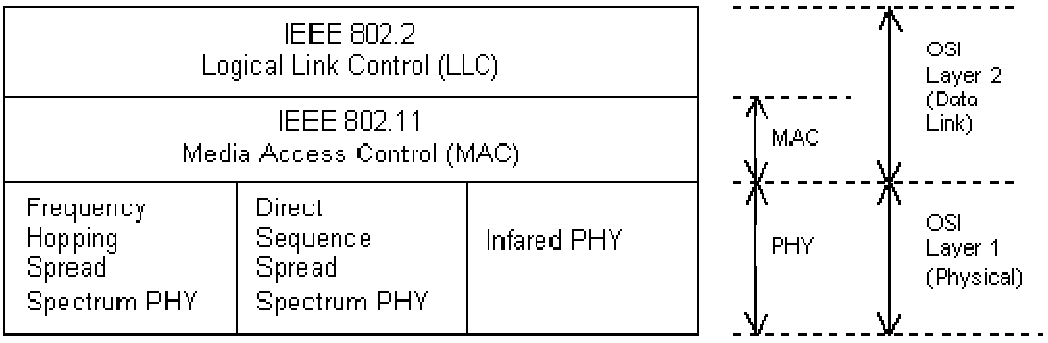


Figure 1. IEEE 802.11 standards mapped to the OSI reference model.

2.2 The IEEE 802.11 Wireless LAN Architecture

Each computer, mobile, portable or fixed, is referred to as a station in 802.11 [Wireless Local Area Networks]. The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement. When two or more stations come together to communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.

A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

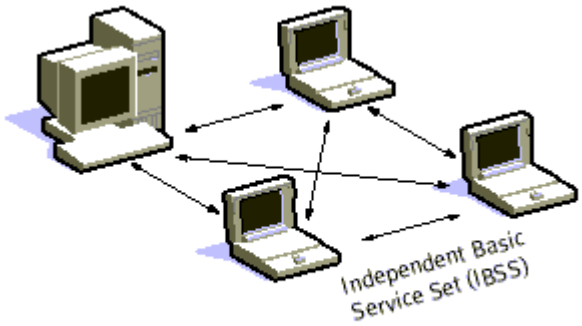


Figure 2. Adhoc Mode

When multiple BSS are interconnected the network becomes one with infrastructure. 802.11 infrastructure has several elements. Two or more BSS are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points.

Creating large and complex networks using BSS and DS lead us to the next level of hierarchy, the Extended Service Set or ESS. The feature of the ESS is that the entire network looks like an

independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS transparently to the LLC.

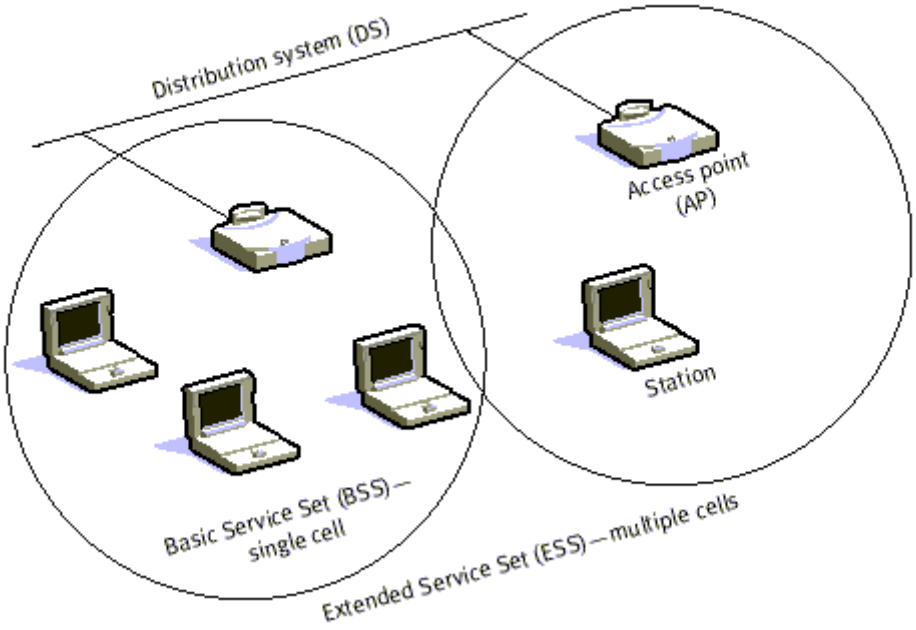


Figure 3. Infrastructure Mode

One of the requirements of IEEE 802.11 is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS. All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as bridge between wired and wireless.

The implementation of the DS is not specified by 802.11. Therefore, a distribution system may be created from existing or new technologies. A point-to-point bridge connecting LANs in two separate buildings could become a DS.

While the implementation for the DS is not specified, 802.11 does specify the services, which the DS must support. Services are divided into two sections

1. Station Services (SS)
2. Distribution System Services (DSS).

There are five services provided by the DSS

1. Association
2. Reassociation
3. Disassociation
4. Distribution
5. Integration

The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the stations mobility is termed No-transition. If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSSes of differing ESSes it is ESS transition. A station must affiliate itself with the BSS infrastructure if it wants to use the LAN. This is done by associating itself with an access point. Associations are dynamic in nature because stations move, turn on or turn off. A station can only be associated with one AP. This ensures that the DS always knows where the station is.

Association supports no-transition mobility but is not enough to support BSS-transition. Reassociation service allows the station to switch its association from one AP to another. Both

association and reassociation are initiated a station. Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party. A disassociated station cannot send or receive data. ESS-transition is not supported. A station can move to a new ESS but will have to reinitiate connections. Distribution and Integration are the remaining DSSes. Distribution is simply getting the data from the sender to the intended receiver. The message is sent to the local AP (input AP), then distributed through the DS to the AP (output AP) that the recipient is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same. So the distribution service is logically invoked whether the data is going through the DS or not. Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS. Station services are:

1. Authentication
2. Deauthentication
3. Privacy
4. MAC Service Data Unit (MSDU) Delivery.

With a wireless system, the medium is not exactly bounded as with a wired system. In order to control access to the network, stations must first establish their identity. This is like entering a radio net in the military.

Before a station is acknowledged and allowed to converse, it must first pass a series of tests. The station is recognized by its own identity. This service is called authentication. Once a station has been authenticated, it may then associate itself. The authentication relationship may be between two stations inside an IBSS or to the AP of the BSS. Authentication outside of the BSS does not take place.

There are two types of authentication services offered by 802.11. The first is Open System Authentication. This means that anyone who attempts to authenticate will receive authentication. The second type is Shared Key Authentication. In order to become authenticated the users must be in possession of a shared secret key. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret key is delivered to all stations ahead of time in some secure method.

Deauthentication is when either the station or AP wishes to terminate a station's authentication. When this happens the station is automatically disassociated. Privacy is an encryption algorithm, which is used so that other 802.11 users cannot eavesdrop on the LAN traffic. IEEE 802.11 specifies WEP as an optional algorithm to satisfy privacy. If WEP is not used then stations are "in the clear" or "in the red", meaning that their traffic is not encrypted. Data transmitted in the clear are called plaintext. Data transmissions, which are encrypted, are called ciphertext. All stations start "in the red" until they are authenticated. MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points.

Authentication is basically a network wide password. Privacy is whether or not encryption is used. WEP is used to protect authorized stations from eavesdroppers. WEP is reasonably strong. The algorithm can be broken in time. The relationship between breaking the algorithm is directly related to the length of time that a key is in use. WEP allows for changing of the key to prevent brute force attack of the algorithm. WEP can be implemented in hardware or software. One reason that WEP is optional is because encryption may not be exported from the United States. This allows 802.11 to be a standard outside the U.S. without the encryption.

The 802.11 family currently includes six over-the-air modulation techniques that all use the same protocol, the most popular techniques are those defined by the a, b, and g amendments to the original standard; security was originally included, and was later enhanced via the 802.11i amendment. Other standards in the family (c–f, h–j, n) are service enhancement and extensions, or corrections to previous specifications. 802.11b was the first widely accepted wireless networking standard, followed by 802.11a and 802.11g.

802.11b and 802.11g standards use the unlicensed 2.4 Gigahertz (GHz) band. The 802.11a standard uses the 5 GHz band. Operating in an unregulated frequency band, 802.11b and 802.11g equipment can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz band.

2.3 IEEE 802.11 Standards

The following standards and task groups exist within the working group:

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11d - International (country-to-country) roaming extensions New countries
- IEEE 802.11e - Enhancements: QoS, including packet bursting
- IEEE 802.11F - Inter-Access Point Protocol (IAPP)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - 5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) and Transmit Power Control (TPC) for European compatibility
- IEEE 802.11i (ratified 24 June 2004) - Enhanced security

- IEEE 802.11j - Extensions for Japan
- IEEE 802.11k - Radio resource measurements
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - Wireless mesh networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management

2.4 The WEP Protocol

WEP is part of the IEEE 802.11 standard (ratified in September 1999), and is a scheme used to secure wireless networks (WiFi). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was designed to provide comparable confidentiality to a traditional wired network, hence the name.

WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to

another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

WEP is 802.11's optional encryption standard implemented in the MAC Layer that most radio network interface card (NIC) and access point vendors support. These standards have been accepted by the industry; related hardware is available and is in widespread use.

The WEP algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe; however, no commercial system we are aware of has mechanisms to support such techniques.

The IEEE 802.11 standards have been described in detail in [3]. In this section we review the key points of the WEP protocol followed by a comprehensive description of the WEP. IEEE 802.11 defines a mechanism for encrypting the contents of 802.11 data frames.

2.4.1 The WEP mechanism

WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce ciphertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext.

This mode of operation makes stream ciphers vulnerable to several attacks. If an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical as more ciphertexts that use the same key stream are known. Once one of the plaintexts becomes known, it is trivial to recover all of the others.

WEP has defenses against both of these attacks. To ensure that a packet has not been modified in transit, it uses an Integrity Check (IC) field in the packet. To avoid encrypting two ciphertexts with the same key stream, an Initialization Vector (IV) is used to augment the shared secret key and produce a different RC4 key for each packet. The IV is also included in the packet. However, both of these measures are implemented incorrectly, resulting in poor security.

The integrity check field is implemented as a Cyclic Redundancy Check-32 (CRC-32) checksum, which is part of the encrypted payload of the packet. However, CRC-32 is *linear*, which means that it is possible to compute the bit difference of two CRCs based on the bit

difference of the messages over which they are taken. In other words, flipping bit n in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message. Because flipping bits carries through after an RC4 decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.

The IV in WEP is a 24-bit field, which is sent in the cleartext part of a message. Such a small space of initialization vectors *guarantees* the reuse of the same key stream. 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. (The amount of time may be even smaller, since many packets are smaller than 1500 bytes.) This allows an attacker to collect two ciphertexts that are encrypted with the same key stream and perform statistical attacks to recover the plaintext. Worse, when the same key is used by all mobile stations, there are even more chances of IV collision. For example, a common wireless card from Lucent resets the IV to 0 each time a card is initialized, and increments the IV by 1 with each packet. This means that two cards inserted at roughly the same time will provide an abundance of IV collisions for an attacker.

In the first and foremost stage each member of the Basic Service Set (BSS) is initialized with a shared secret key *K,* (The details of initialization are not known. It could be either end user contacting the network administrator for the shared key or network administrator distributing the keys to the legitimate user). Before sending the frame the sender calculates the (CRC) of the frame payload and appends it to the frame, which now becomes the plaintext.

Encryption: The frame is encrypted using RC4 algorithm [7]. A new IV is chosen and is appended to the shared key *K* to form a "per-packet" key. This is now used to generate a RC4 key schedule. The sender uses RC4 to generate a key stream equal to the length of the plaintext. The sender XORs the generated key stream against the plaintext. This now becomes the cipher text. The sender also sends the value of the IV in the unencrypted portion of the frame and sends a Key ID # which enables the user to identify which shared key he has to use to decrypt the frame. An appropriate bit is set in the frame header to indicate that it is WEP encrypted packet. Figure. 4 describes the frame structure to be transmitted to the wireless node (receiver).

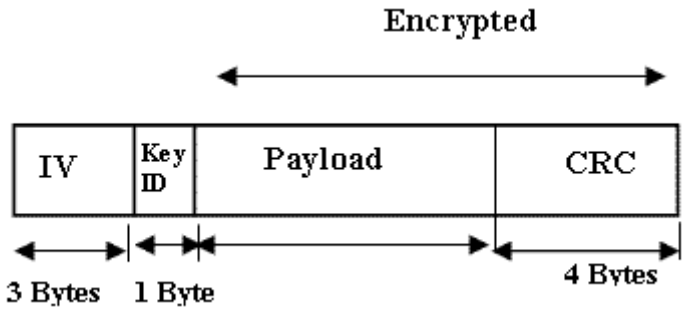


Figure 4. The WEP Frame Structure

Decryption: The decryption process works fairly the same as encryption but the reverse way. The receiver checks the encrypted bit in the WEP frame. If it is enabled he takes out the IV and uses with his shared key to generate an RC4 key schedule. RC4 is applied to the key schedule to generate a key stream equal to the length of the encrypted payload from the frame. The receiver then XORs this key stream with the encrypted payload to get the plaintext. Finally, the receiver checks the CRC of the obtained plaintext to verify that the frame data was correctly sent.

2.4.2 Details of RC4 Algorithm

The RC4 encryption algorithm is stream cipher, which can use variable length keys. The algorithm was developed in 1987 by Ron Rivest, for RSA Data Security, and was a propriety algorithm until 1994. RC4 (or ARCFOUR) is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks). RC4 falls short of the high standards of security set by cryptographers, and some ways of using RC4 lead to very insecure cryptosystems (including WEP). It is not recommended for use in new systems. However, some systems based on RC4 are secure enough for practical use.

RC4 generates a pseudorandom stream of bits (a "keystream") which, for encryption, is combined with the plaintext using XOR as with any Vernam cipher; decryption is performed the same way. To generate the keystream, the cipher makes use of a secret internal state which consists of two parts:

1. A permutation of all 256 possible bytes (denoted "S" below).
2. Two 8-bit index-pointers (denoted "i" and "j").

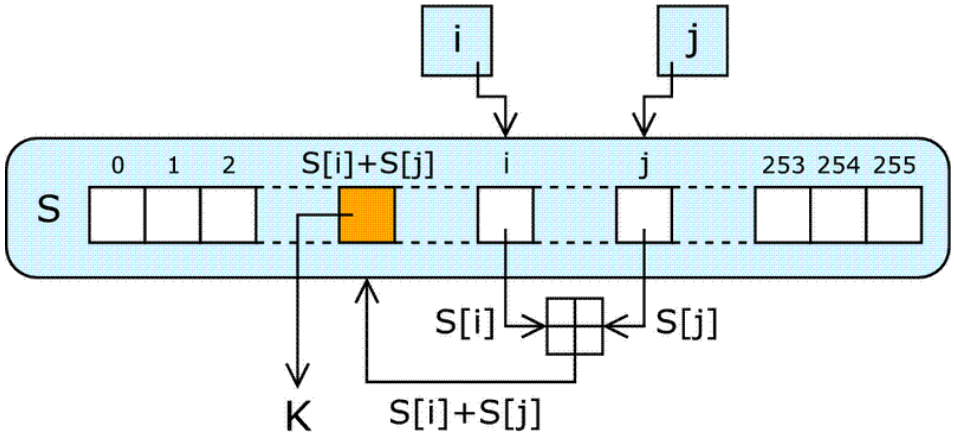
The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA). Once this has been completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

2.4.3 The pseudo-random generation algorithm (PRGA)

For as many iterations as are needed, the PRGA modifies the state and outputs a byte of the keystream. In each iteration, the PRGA increments i, adds the value of S pointed to by i to j,

exchanges the values of S[i] and S[j], and then outputs the value of S at the location S[i] + S[j] (modulo 256). Each value of S is swapped at least once every 256 iterations.

```
i := 0
j := 0
 while GeneratingOutput:
     i := (i + 1) mod 256
     j := (j + S[i]) mod 256
     swap(S[i],S[j])
     output S[(S[i] + S[j]) mod 256]
```



The output byte K is the content of element of S where the index of the element is computer by adding modulo 256 the values of S(i) and S(j).

2.4.4 The key-scheduling algorithm (KSA)

The key-scheduling algorithm is used to initialize the permutation in the array "S". "i" is defined as the number of bytes in the key and can be in the range $1 \leq i \leq 256$, typically between 5 and 16, corresponding to a key length 0–128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA algorithm, but also mixes in bytes of the key at the same time.

```
for i from 0 to 255
     S[i] := i
 j: = 0
 for i from 0 to 255
     j := (j + S[i] + key[i mod l]) mod 256
     swap(S[i],S[j])
```

Implementation:

Many stream ciphers are based on linear feedback shift registers (LFSRs), and, while efficient in hardware, are much slower in software. The design of RC4 is quite different and is ideal for software implementations, as it requires only byte-length manipulations. It uses 256 bytes of memory for the state array, S[0] through S[255], n bytes of memory for the key, key[0] through key[n-1], and integer variables, i, j, and k. Performing a modulus 256 can be done with a bitwise AND with 255 bytes.

2.5 Security

RC4 falls short of the standards set by cryptographers for a secure cipher in several ways, and thus is not recommended for use in new applications. The keystream generated by RC4 is slightly biased in favour of certain sequences of bytes. The best attack based on this bias is due to Fluhrer and McGrew, which will distinguish the keystream from a random permutation given a gigabyte of output.

RC4 does not take a separate nonce alongside the key. As with any cipher, but particularly with Vernam ciphers, such a nonce is a requirement for security, so that encrypting the same message twice produces a different ciphertext each time. A secure solution to this that works for any secure cipher is to generate each RC4 key by hashing a long-term key with a unique nonce using a construction such as HMAC. However, many applications that use RC4 simply concatenate key and nonce; RC4's weak key schedule then gives rise to a variety of serious problems.

2.6 Security Flaws in WEP

WEP has considerable flaws in mechanisms including authentication, replay prevention, message modification detection, and most importantly key protection and message privacy [1, 6]. In this section we focus mainly on WEP's weaknesses in handling message privacy because this is of priori importance. If an attacker can break the encryption method and get the key he can go unnoticed and actually use the network to perform malicious activities. There are few flaws in the way RC4 has been used in the WEP and this has made the WEP vulnerable to attackers [1, 2 and 4]. We enumerate the flaws of the WEP.

IV Reuse Attack: In section 2.4.1 we describe the WEP protocol mechanism. In this section we delve into the intricacies about how IV is used in the WEP. Instead of using fixed secret key WEP appends the secret key to the 24-bit IV value. The combined IV and secret key is used as an encryption key. Effectively we have a different key for every transmitted frame. There can be 2^{24} different IVs and we don't intend to reuse the IV with the same shared secret key because that would help an attacker break the key [1, 4]. If we choose IVs randomly there is a good chance of reusing the same IV with the same-shared key due to the "Birthday Attack" [9]. Another way in which different IVs can be derived is to start the value of IV from 0 and increment it by 1 till we reach (2^{24}-1). A single access point BSS running at 11Mbps with a typical packet distribution can exhaust the derived key space in just a couple of hours. Therefore, we always run a risk of exhausting our IVs [4]. The consequence of this is enough samples of duplicated IVs that can help the attacker guess good amount of portions of the key stream making the decoding relatively easier [6].

RC4 Weak Keys: Fluhrer et al. [2] states that the way WEP uses RC4 creates subtle weaknesses. They have proved that for certain "weak" keys a disproportionate number of bits in the first few bytes of the key stream (pseudorandom bytes) are determined by a few bits in the key itself [2]. In the WEP first few bytes are the LLC headers that always start with the same hexadecimal value of "AA". So if you know the plaintext, you can derive the key stream and start attacking the key. These flaws have become an area of major concern.

Direct Key Attacks: Fluhrer et all showed that using a public IV value appended to the secret key generated a huge weakness because it allowed the attacker to wait for a potentially weak key and directly attack the key. There are two cases, one in which IV is appended and one in which the IV is prepended. The prepend case is the more vulnerable and is the relevant case for WEP. This attack is based on exploiting the weak key problems in the first bytes. First few bytes of an 802.11 WEP frame are LLC SNAP header. An attacker can look for a weak key generated by the IV. Since we know that there is correlation between the ciphertext, the plaintext and the secret key bytes, there are only a limited number of possible values for the first secret key byte that could match the plaintext and ciphertext. After capturing about 60 such messages an attacker can guess the first key byte with reasonable certainty.

The method can be tuned to attack each secret key byte in turn so eventually the entire secret key can be extracted. Increasing the key size from 40 bits to 104 bits only means that it takes 2.5 times longer to extract the key – in other words, the time to crack the key goes up linearly with key sizes rather than exponentially.

2.7 Key management and key size

Key management is not specified in the WEP standard; without interoperable key management, keys will tend to be long-lived and of poor quality. Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access points and client stations must be programmed with the same WEP key. Since synchronizing the change of keys is tedious and difficult, keys are seldom changed. Also, the 802.11 standard does not specify any WEP key sizes other than 40 bits.

CHAPTER THREE: PREVIOUS WORK ON IMPROVING WEP

Over the years many types of attacks have been identified on WEP. The research community tried to propose and eliminate the problems associated with WEP. Some proposed minor changes in the WEP protocol design and some said to reconsider its design. Walker [4] was the first one to identify the weaknesses in the WEP. He has mentioned the WEP IV problems and usage of RC4 algorithm in his important paper. He proposed not to use RC4 stream cipher for WEP environment and instead pushed the use of more secure ciphers such as AES in Offset Codebook Mode (OCB). He also stresses on session key derivation. Chandran et all [11] propose a mechanism called Variable Encryption Function (VEF) to enhance the protection offered by WEP. The VEF mechanism is based on increasing the 'diffusion' characteristic, at the application layer, by making the ciphertext character dependent on the current plaintext character and the previous plaintext character. A message dependent matrix is generated which is used to perform the transposition operation on the obtained ciphertext. Nancy Cam-Winget et all [14] proposed to have longer IVs (128 bits). They also proposed to derive WEP key from Master key and change encryption key frequently. They went on to explain Key management which was soon going to be a part of WPA.

Over the years following enhancements have been tried on WEP to save it from the flaws it has in its design.

1. Cipher Mode of operation: All new symmetric key encryption efforts starting now should be based on the AES [15] block cipher. It is thought to be as good as any symmetric key cipher in the public domain, and allows for very efficient implementations over a very wide range of

environments (8-bit processors to super computers). The reformulated WEP should instead employ 128-bit AES as the mandatory to implement cipher.

Also recommended was to use WEP with AES in Offset Codebook Mode. This is a stream cipher that also produces a message authentication code, preventing an adversary from forging messages. The data encrypted under OCB is the same length as the plaintext data, a single key is used for both encryption and authentication, and it requires only the AES encryption, not decryption, engine. It is also a parallelizable mode, allowing for very high throughput. OCB has been optimized to minimize the number of calls to lower level cryptographic primitives, and can both encrypt/decrypt and tag/verify a message in a single pass.

The OCB state is the key, a stride, which provides the offset in the mode's name, and an IV. The stride and the IV are of the cipher block size (128 bits for AES). The stride is computed once per session. The per-frame overhead of OCB is 128 bits for the IV, and 128 bits for the OCB authentication tag.

2. **Session Key Derivation**: J.Walker [4] recommends a session key derivation algorithm in the case of a manually configured base key, as used by WEP today. It does not recommend an algorithm for session key derivation when dynamic keying is available, because the scheme should incorporate state from the dynamic keying operation, to tie the key to the particular session that negotiated the key.

This algorithm produces two session keys, one for sending and the other for receiving.

i. Concatenate the (a) BSSID, (b) the sender's MAC address, and (c) the receiver's MAC address to produce a string. The order is important, as the two MAC addresses are reversed for sending and receiving.

ii. Using the base key (manually configured key) and an IV of 128 zero bits, run the OCB-AES algorithm on the concatenated string. The session key is the authentication tag output by this:

session-key ← OCB-AES-$tag_{base\text{-}key}$(0, *BSSID* | *sender-mac-addr* | *receiver-mac-address*)

Here '*a* | *b*' means the concatenation of strings *a* and *b*.

The motives for this algorithm are (a) to remove the base-key from direct attack and (b) weakly tie the session key to the particular parties using it. Under this algorithm different sets of peers use different session keys, even though all the members of the BSS share the same base key. Note that the keys produced by this algorithm are still subject to dictionary attack when the base key is a password or derived from a password by techniques such as PCKS #5. And all the keys are subject to spoofing if the base key is revealed to an adversary. There is no magic that can avoid these weaknesses.

3. Random data: The security of the recommended scheme depends critically on a source of cryptographically secure random numbers. Implementations must appear to produce random numbers for their nonces, even across power cycles and reboots.

4. Encapsulation: J Walker also proposed a new WEP encapsulation.

i. A 128-bit IV. At session initiation the encrypter selects this randomly. On subsequent frames the encrypter may use the last 128-bits of encrypted data from the previous encrypted frame.

ii. A 32-bit sequence number. This will be the first quantity encrypted. It indicates the number of frames sent under the present key. When manual keys are used, the sequence

number is not used and set to 0. When dynamic keys are used, it is initialized to zero when the key is established.

iii. The LLC data payload. This will also be encrypted.

iv. The 128-bit OCB data authentication tag.

The encapsulation scheme thus adds 36 bytes to the frame size. This is the cost of privacy in a network these days.

To WEP encapsulate a frame, the encrypter first checks that the counter has not yet assumed the maximum value. If it has, the data stream encrypted under the present key terminates until the key management system replaces the base key. If the counter has not yet assumed its maximum value, and if dynamic keys are used, the encrypter increments the counter by 1 and inserts the new counter value into the appropriate location in the frame. The encrypter then selects the nonce and OCB encrypts/tags the counter and data. It inserts the OCG authentication tag at the tail of the frame. The frame is now ready to transmit.

To WEP decapsulate a received frame, the decryptor locates the correct context by the arriving MAC address. It uses the IV from the frame to OCB decypt the packet and verify its authenticity. If the session is dynamically keyed, it finally verifies that the counter is greater than any prior received value, i.e., the WEP receiver maintains a receive window size of 1. This prevents replay attack in the case when the session is dynamically keyed. Replay prevention is not feasible without dynamic keying.

5. Variable Encryption Function: Chandran et all [11] proposed a VEF scheme to make WEP more secure. The Variable Encrypting Function (VEF) mechanism is based on increasing the

'diffusion' characteristic, using block chaining algorithm at the application layer, by making the ciphertext character dependent on the current plaintext character and the previous plaintext character. This mechanism consists of a table having 128 permutations of the numbers 0 to 127. These permutations are indexed in a particular order. Depending on the ASCII value of the previous character of the plaintext, the corresponding permutation is selected. The encrypted character is obtained by using this permutation and the current ASCII character of the plaintext. Including the dependence of previous characters ensures that 'sniffing' of frames in-between transmissions would be ineffective.

6. Longer IVs: Winget et all [14] proposed to use longer IV bits. They stressed on 128 bit IV to withstand IV attacks.

In the next chapter we show our proposed new WEP frame architecture and also develop an IV collision avoidance algorithm to help save WEP's privacy.

CHAPTER FOUR: OUR PROPOSED METHODOLOGY

In order to overcome the above-mentioned flaws we propose a modification in the current WEP protocol. The idea is to update the shared secret key between the access point and the wireless nodes. The update procedure depends on the following parameters.

1. Network Traffic
2. Number of transmitted frames.

From Borisov et al [1] we always run a risk of repeating IVs after 5000 frames due to birthday paradox [9]. To ensure IV is not reused we use these parameters namely network traffic and number of transmitted frames to change our shared secret key. For example, we can have a WEP system where after every 5000 frames shared secret key is changed. Network traffic determines the number of transmitted WEP frames and that is why these two parameters are important in determining when to change the shared secret key. Our aim is to minimize the information that an attacker can retrieve from the transmitted frames and minimize time available to him to launch an attack.

Access point creates the key mapping for the clients; it can use the MAC addresses of the client to generate the new-shared secret key. The structure of the new WEP frame is as shown in Figure 5,

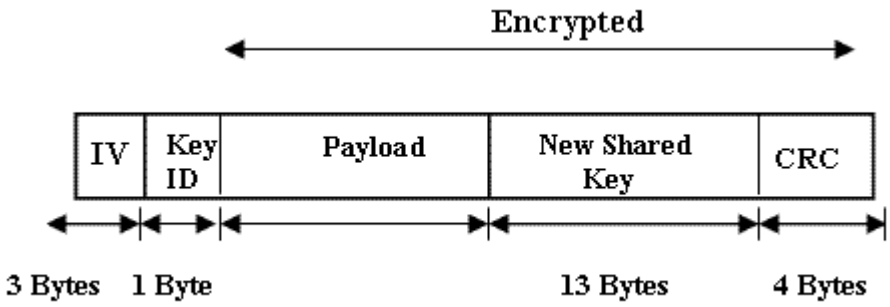


Figure 5. Proposed WEP Frame Structure

In the conventional WEP frame Key ID field signifies which key out of the four possible keys is used to decrypt the current frame. Key IDs are from 0 to 3. Whenever the value of the Key ID field is greater than 3, one needs to subtract 4 from that key ID value to get the correct key to decrypt the current frame. Whenever the Key ID is greater than 3 it would indicate that the data payload is carrying the new-shared key for future encryptions. For example, if the Key ID is 6 it would mean that the receiver has to use the original Key ID = (6 – 4) = 2 for decrypting the current frame. In this case this is an indication for the receiver that this frame has new shared secret key in its payload i.e. last 104 bits of the data payload before 32 bit CRC is the new shared key for future encryptions. Out of the four keys this new-shared secret key will replace the first one. On subsequent updates it will replace the second key, third key and so on. At a given point of time we have 4-shared keys and new shared keys arrive at regular intervals and replace the old ones. Data Payload will be as usual except that it makes provision for extra 104 bits when the new shared secret key is being sent. When the receiver decrypts the frame it takes out the last 104 bits in the data payload and uses them as the shared secret key for future encryptions.

There are two different approaches to using keys under WEP; these are default keys and key mapping keys [6]. In the default keys all the wireless nodes and access points have the same set of shared secret keys while in the case of key mapping keys every individual wireless node has different set of shared secret keys. Default keys are easier to use and are widely used. The key mapping keys are more secure but are difficult for access points to handle. If there are large numbers of wireless nodes connected through an access point, it is difficult for an access point to keep track of the secret keys of all the wireless nodes. In the following section we have discussed updating mechanism of shared secret keys for both the cases.

A Default Key

If the system is using default keys, then access point will transmit the new-shared secret key for the future encryptions in the data payload. Since in the case of default keys all wireless nodes are using the same set of shared keys, we will need to update our shared secret keys more often. We use parameters like network traffic or number of frames transmitted for changing our shared secret key so that we do not reuse the IV for the same shared key. If a node is idle it will receive the updated shared secret key from the access point in the usual WEP frame but it won't transmit any other data in it. Key ID field can be used to signify that this frame is carrying a new-shared key for the future encryptions.

B Key Mapping Key

In this type of system the access point will send the new-shared secret key only to the concerned individual node. Having more shared secret keys would help the system stay with the shared keys for longer as it takes more time to exhaust the IVs. The access point can generate the keys for individual nodes using the MAC addresses of the client cards.

Widely used WEP system mainly works with the default key type system but it has 4 pre-stored keys that can be used interchangeably to thwart IV attack on the WEP system. However, using 4 keys is only 4 times more secure and an attacker has to be patient for that much extra time. It doesn't guarantee a near complete security. While in our case regular updating of shared keys ensures that no IVs are being repeated with the same shared key. Thus, our method takes care of the IV reuse attacks.

4.1 IV Avoidance Algorithm

The WEP protocol suffered from several limitations like the IV reuse and weak RC4 keystream reuse attack as discussed in previous section. We tried to eliminate the IV reuse problem by updating the shared key as an enhancement to the existing WEP protocol. From Borisov et all. [1] we see that even if we use random values for IVs we need on average 5000 WEP frames for IVs to collide. In the proposed WEP protocol we change our shared secret key approximately after 5000 frames. But there is always a chance of an IV reuse due to Birthday Paradox. Thus, the IV collision still remains a critical issue and cannot be ignored.

In the following section we propose an IV Collision Avoidance Algorithm that further strengthens our proposed new protocol and makes it foolproof.

1. The key idea in avoiding IV collision is to assign a unique pattern of bits to every wireless node in the system. The AP partitions the IV by choosing specific bits out of the 24 bits in the IV. AP chooses specific bits in order to avoid a predictable pattern.

For e.g. consider an IV of 6 bits. The AP partitions the IV using a specific bit pattern say (1 and 3). The remaining bits (2, 4, 5 and 6) form the other partition and can assume all possible 2^4 = 16 values. The (1 and 3) pattern is unique to all the nodes. Howsoever, the values corresponding

to these bit numbers vary in all possible 2^2= 4 nodes. These variations ensure that even if other partition bits assume the same values the possibility of collision is completely eliminated.

2. The above mentioned pattern will remain intact for a session and will be unique to each node to avoid IV reuse.

3. The AP communicates to each individual node by sending bits equal to (length of IV+ length of the partition number of bits). For e.g. in our case (24+N) bits following the data payload in the WEP frame structure where N is length of partition number of bits. The bits enabled in the first 24 bits will denote that they are partition bits and the remaining N bits will denote the values for that corresponding partition. For e.g. In an IV of 6 bits if the partition is (1, 3) and the corresponding value at these bit positions is (0 and 1) the AP will send a frame of (6+2) = 8 bit (101000, 01).

4. This pattern is transferred only once when the wireless node joins the access point. The pattern holds no good after the wireless node is disconnected from the network. Upon re-association a new pattern is provided by the access point.

The AP by ensuring that no bits at its pre determined pattern are repeated guarantees a complete security.

For example, if the IV length is of 4 bits and we partition it by using 2 bits. Upon joining a network the access point sends the wireless node a pattern of following sequence numbers (0101, 01). This pattern is randomly chosen by the access point and is unique to every node. This would mean that that out of the 4 bits in the IV, bit numbers 2 and 4 are the partition bits since they are enabled and their values are 0 and 1 respectively which is shown by the two rightmost bits in the pattern as shown in the above figure.

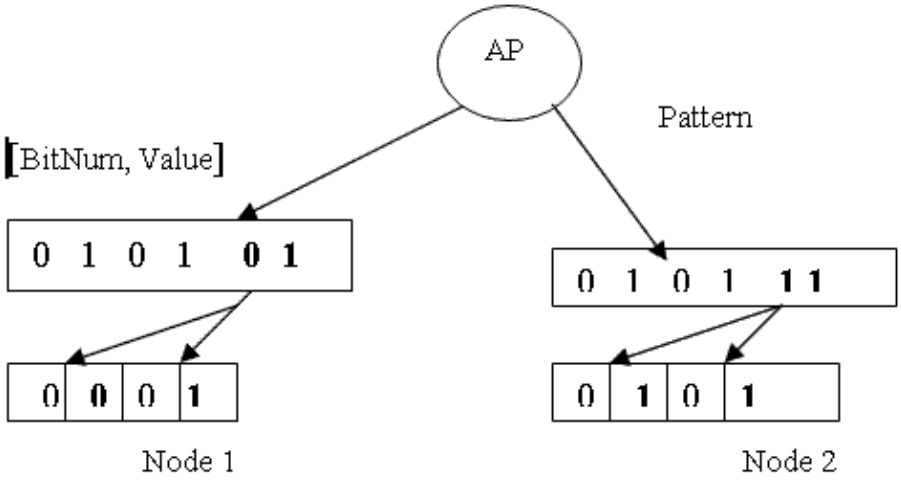


Figure 6: IV structure with bits enabled

Figure 6 shows bits enabled corresponding to the partition bits in the pattern. The remaining 2 bits can generate 2^2 different IVs without collision. It can increment the 2 bits in every IV making sure that we follow a simple pattern of incrementing bits in the remaining 2 bits and do not reuse any IV. Thus, we take care of IV collision by generating a pattern of sequence numbers unique to each node.

Nodes	Node1	Node2	Node 3	Node4
Partition1 [2,5], 2^2=4	1 **2** 3 4 **5**	1 **2** 3 4 **5**	1 **2** 3 4 **5**	1 **2** 3 4 **5**
Constant Bit Values	**0 0**	**0 1**	**1 0**	**1 1**
Partition2 [1,3,4] , 2^3=8	0 **0** 0 0 **0**	0 **0** 0 0 **1**	**1** 0 0 0 **0**	0 **1** 0 0 **1**
	0 **0** 0 1 **0**	0 **0** 0 1 **1**	**1** 0 0 1 **0**	0 **1** 0 1 **1**
	0 **0** 1 0 **0**	0 **0** 1 0 **1**	**1** 0 1 0 **0**	0 **1** 1 0 **1**
	0 **0** 1 1 **0**	0 **0** 1 1 **1**	**1** 0 1 1 **0**	0 **1** 1 1 **1**
	1 **0** 0 0 **0**	1 **0** 0 0 **1**	**1** 1 0 0 **0**	1 **1** 0 0 **1**
	1 **0** 0 1 **0**	1 **0** 0 1 **1**	**1** 1 0 1 **0**	1 **1** 0 1 **1**
	1 **0** 1 0 **0**	1 **0** 1 0 **1**	**1** 1 1 0 **0**	1 **1** 1 0 **1**
	1 **0** 1 1 **0**	1 **0** 1 1 **1**	**1** 1 1 1 **0**	1 **1** 1 1 **1**

Figure7: Possible IV Combinations used by each node

4.2 Access Point Key Management System

Our proposed method relies on updating the shared secret key. Thus it necessitates an efficient key management system on the part of the access point. In this section we suggest a framework for the access point key management system to further enhance the efficiency of the proposed protocol.

The proposed method makes an implicit assumption that the nodes on joining the network have already procured the key through authentication means and are legitimate users. Also, the communication link is error free and all the communication via the access point to the intended user is received in time. Transit times for keys are constant for all the nodes in the system.

At an arbitrary time T in the system the Access Point distributes the new updated keys to all the nodes. Nodes upon receiving the keys respond by acknowledging the receipt of the key. The primary function of the access point is to keep track of the nodes that have received the new keys by monitoring the acknowledged frames. The access point distributes a pattern of sequence number to every node in the system. It ensures this pattern is unique to each node which helps eliminate IV reuse. Thus, the access point management system is pivotal to the efficiency of our proposed protocol.

CHAPTER FIVE: ANALYSIS

Our proposed technique proves to be better than the existing methods as it withstands the IV reuse attacks efficiently. Since shared keys are changed after every few thousand frames the chance of reusing the same IV is minimal. Even if an attacker finds a shared key using same IVs, which is highly improbable, by the time he detects it and launches an attack there will be a new-shared secret key in the system. In our case since we are updating secret key so often the probability of an IV being reused with the same secret key is $(1/ 2^{128})$. This makes the IV reuse attack extremely difficult for an attacker.

The WEP IV space is far too small; to give reader an idea J.R.Walker [2] has mentioned that we exceed a 50% chance of colliding IVs only after transmitting 4823 frames owing to the Birthday Paradox. For example if we perform some calculations we see that a busy access point sending 1500 byte packets and achieving an average 5 Mbps bandwidth will transmit 3500 frames per second.

Number of Frames transmitted / sec

= (5 Mbps/1500 bytes)

= 3495 (3500 approx.)

If we adhere to change of IV after every 5000 frames in order to avoid IV reuse with the same shared key, the time required between the key changes is 1.42 seconds. Table 1 below shows the frequency with which we change our keys depending upon the bandwidth and number of frames transmitted.

Table 1. Time Evaluation between key changes [Varying Bandwidth]

Average Bandwidth	**#of Frames transmitted in one second**	**Time$^{\Psi}$ between the key changes**	**Time$^{\pi}$ available to attacker**
1 Mbps	700	7.14 sec	6.66 hrs
2 Mbps	1400	3.57 sec	3.33 hrs
3 Mbps	2100	2.38 sec	2.21 hrs
5 Mbps	3500	1.42 sec	1.33 hrs
7 Mbps	4900	1.02 sec	0.95 hrs
11 Mbps	7700	0.65 sec	0.60 hrs

Table 1 highlights the comparison between the times available to an attacker in the conventional WEP as against our proposed method. For this evaluation we have varying bandwidths with a utilization factor of 1.0. For e.g.

Let T = Time available to a attacker,

N = Number of Frames = 3500

Consider in the conventional WEP the shared secret key changes only after exhausting all possible 2^{24} IVs then,

$T = 2^{24}/ N = 16777216 / 3500$ sec = 1.33 hours

$^{\Psi}$ Time available to an attacker in Proposed WEP
$^{\pi}$ Time available to an attacker in Conventional WEP

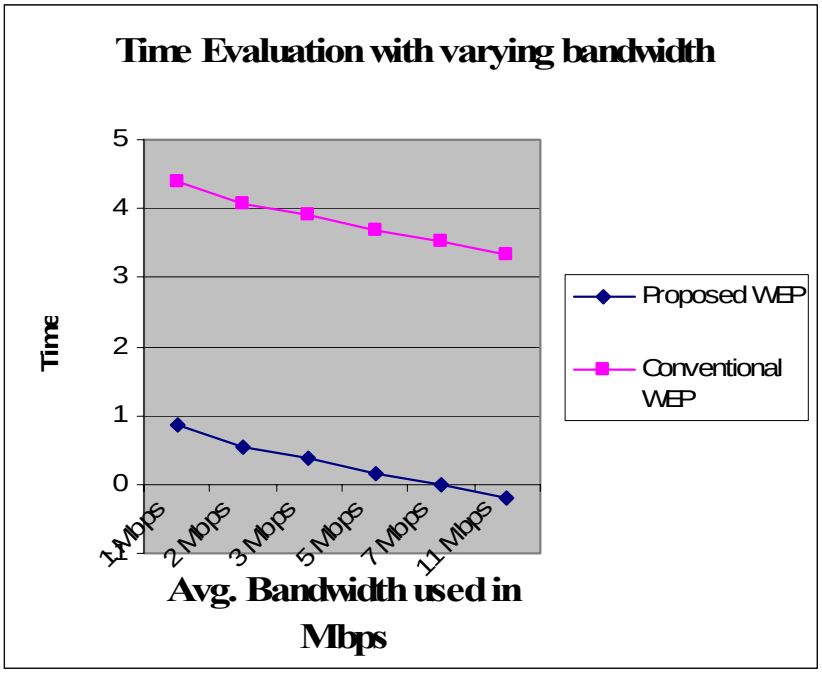


Figure 8. Log of Time in sec v/s Avg Bandwidth

In our method we calculate time T by changing the shared secret key after 5000 frames.

T = 5000/3500 sec = 1.42 sec.

Table 2. Time Evaluation between key changes [Varying Network Load]

# of Frames transmitted per second	**Time$^{\Psi}$ between the key changes**	**Time$^{\pi}$ available to attacker**
500	10.0 sec	9.32 hrs
1000	5.0 sec	4.66 hrs
1500	3.33 sec	3.11 hrs
2000	2.5 sec	2.33 hrs
2500	2.0 sec	1.86 hrs
3000	1.66 sec	1.55 hrs
3500	1.42 sec	1.33 hrs
4000	1.25 sec	1.16 hrs
4500	1.11 sec	1.03 hrs
5000	1.00 sec	0.93 hrs
10000	0.5 sec	0.466 hrs
20000	0.25 sec	0.233 hrs

Table 2 shows time evaluation considering constant bandwidth (say 54 Mbps) and varying loads on the network (frames/sec). The bandwidth utilization factor is considered to be varying and less than 1. Computations are similar to those in Table 1.

$^{\Psi}$ Time available to an attacker in Proposed WEP
$^{\pi}$ Time available to an attacker in Conventional WEP

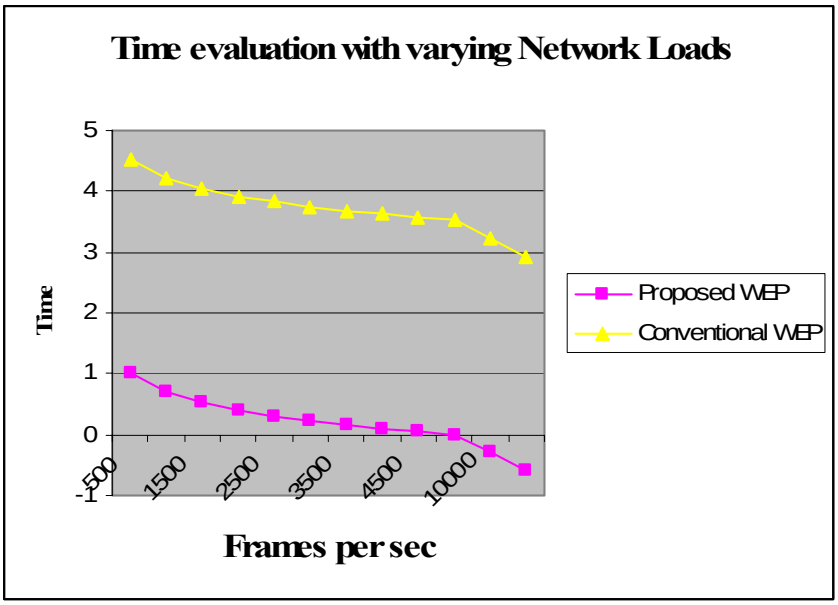


Figure 9. Log of Time in sec v/s Network Load

It is evident from Figure 8 and Figure 9 that in our proposed method the time available to an attacker is negligible and proves to be more efficient than the conventional WEP.

Moreover, our proposed method also provides a very efficient solution to the RC4 weak key stream attack. Considering the possibility of a weak key RC4 stream in the system, by the time it is actually detected and used a new WEP key in the system is already in and being used. This makes the attack, even if successful, futile. In the nutshell frequent changing of WEP key thwarts all kinds of cryptanalytic attacks.

5.1 IV Collision Analysis

By using our proposed algorithm we successfully eliminate the IV collision problem that persisted in the conventional WEP. We change our shared secret keys after 5000 frames but using our IV avoidance algorithm we ensure that no IV is being reused in these 5000 frames thereby eliminating the security threat associated with the IV reuse.

Out of the possible 24 bits in the IVs we can have K bits for the pattern and remaining (24-K) bits varying thereby generating $2^{(24-K)}$ different IVs by each node. For example if K =8 then we have can have 8 bits for the pattern thereby meaning that we can have $2^8 = 256$ nodes active at one point of time without collision. By incrementing the value of K we can increase the number of active wireless nodes in the network without IV collision. Similarly if K = 9, we can generate 2^{15} different combination of IVs.

We eliminate the IV reuse problem completely by following the IV avoidance algorithm. Thus, our IV avoidance algorithm in addition to the proposed WEP protocol together lays a framework for a strong and secure WEP protocol.

5.2 Overhead Analysis

Shared keys at most take 40 bits (5 bytes) or 104 bits (13 bytes). The size of the WEP frames varies from 10 bytes to 1500 bytes. The shared secret keys are exchanged at time intervals depending on various parameters previously mentioned.

Let the length of the data Payload be L, shared key length be S and K be the number of frames after which we change our shared key. That means, we use S bits out of (K*L) bits for transmitting the new shared key.

Overhead incurred = (100*S) / (K*L) %

As mentioned in J.R.Walker [4] and Borisov et al. [1], there is 50% chance of an IV reuse after transmitting 5000 WEP frames.[£] To avoid the IV reuse we take K= 5000 in the following table.

Table 3: Overhead Incurred by shared keys

L	**Overhead for S = 5 bytes**	**Overhead for S = 13 bytes**
10	0.01 %	0.026 %
50	0.002 %	0.0052 %
100	0.001 %	0.0026 %
200	0.0005 %	0.0013 %
500	0.0002 %	0.00052 %
1000	0.0001 %	0.00026 %
1500	6.67E-05 %	0.00017333 %

In Table 3 we have assumed the shared key size of 104 bits (13 bytes) and 40 bits (5 bytes). The overhead in the 13 byte case is obviously higher than 5 bytes because shared key occupies more space. These results show that the overhead associated with transmitting the shared key is very less and without loss of generality we can say that it has the same performance in terms of space occupied as the original WEP.

5.3 Analysis of hardware upgrade

The vendors can implement the above-mentioned changes in the protocol and a firmware upgrade is required to make complaint to our protocol. No additional hardware changes are needed unlike new systems such as 802.11i [10]. It's still sometime before appropriate hardware is available for 802.11i and till then we can continue to use our existing systems efficiently and in a much more secured way.

£ This result is because of "Birthday Paradox"

CHAPTER SIX: CONCLUSION

Existing WEP protocol has been shown to be vulnerable to different kinds of cryptanalytic attacks [6]. These stem from inappropriate usage of cryptography and not because of the key size.

The possible drawback one can identify with our method is the computational overhead associated with generating, and transmitting the session keys at the access point. In this paper we have shown that our proposed modification to the existing WEP protocol makes it more secure and robust in terms of Message Privacy. The fact that we frequently change the shared secret keys through the WEP mechanism makes any kind of cryptanalytic attack futile. The IV collision problem has been successfully resolved by our proposed IV avoidance algorithm that further enhanced the security of WEP. IEEE 802.11i standards have explicitly talked about key management which is must for its security but comes with the overhead of upgrading the hardware. Our proposed solution is a very efficient alternative till actual hardware is available and deployed for 802.11i. Our proposed system works well with the existing hardware and gives an edge over the present WEP protocol.

REFERENCES

[01] N.Borisov, I. Goldberg, and D.Wagner. Intercepting mobile communications: The insecurity of 802.11. In *MOBICOM 2001*, Rome, Italy, July 2001.

[02] S.Fluhrer, I.Mantin, and A.Shamir. Weaknesses in the key-scheduling algorithm of RC4. In *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada, Aug. 2001.

[03] L.M.S.C of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer specifications. *IEEE Standard 802.11, 1999 Edition*, 1999.

[04] J.R.Walker. Unsafe at any key size; an analysis of the WEP encapsulation. IEEE Document 802.11-00/362, Oct 2000.

[05] W.A.Arbaugh, N.Shankar, and Y.J Wan. Your 802.11 wireless network has no clothes. In *IEEE International Conference on Wireless LANs and Home Networks*.

[06] J.Edney and W.A.Arabaugh, "Real 802.11 Security Wi-Fi Protected Access and 802.11i", 2004, Pearsons Education Inc.

[07] William Stallings, Cryptography and Network Security, Principles and Practices", 3rd Edition, 2003, Pearsons Educations.

[08] A.Stubblefield, J.Ioannaidis, and A.D.Rubin. Using the Fluhrer Mantin and Shamir attack to break WEP. *ACM Transactions on Information and Security Security, Vol. 7, No. 2, May 2004, Pages 319-332*.

[09] http://en.wikipedia.org/wiki/Birthday_attack

[10] http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf

[11] N.Chandran, D.Sampath. Strengthening WEP Protocol for Wireless Networks using Block Chaining Algorithm with Variable Encrypting function Mechanism. *2004 IEEE Sarnoff Symposium on Advances in Wired and Wireless Communications, Princeton, NJ, USA*.

[12] D.Purandare, R.Guha. Enhancing Message Privacy in WEP. To appear in *International Workshop on Wireless Information Systems, ICEIS 2005, Miami USA.*

[13] D.Purandare, R.Guha. An IV Collision Avoidance Algorithm-Strengthening the WEP. To appear in *The 2005 International Conference on Wireless Networks ICWN-05, Las Vegas, Nevada, USA.*

[14] N. Cam-Winget, J.Walker, B.Aboba, J Kubler, A Recommended practice to improve WAN security. IEEE 802.11-00/383 August 2001.

[15] AES Algorithm (Rijndael). http://csrc.nist.gov/CryptoToolkit/aes/rijndael/