International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 5 Issue 2|| February 2016 || PP.35-45

Security Analysis and Improvement for IEEE 802.11i

Nagmden Miled Naser[1], Ali Emhemmad Almosi[2]
[1](*Electrical Engineering and Computer Science Department, Faculty/Al-Mergheb ,Libya)*
[2](*Electrical Engineering and Computer Science Department Faculty/Al-Mergheb ,Libya,)*

Abstract: *While conventional cryptographic security mechanisms are essential to the overall problem, of securing wireless networks, the wireless medium is a powerful source of domain-specific information, that can complement and enhancetraditional security mechanisms .*
In this work a security paradigms, which exploit physical layer properties of the wireless medium, can enhance confidentiality and authentication services.In essence using the physical layer information available , we are able to continuously authenticate packets at the same layer. However ,this form of security is only possible through physical layer security mechanisms.
An approach where wireless devices, interested in establishing a secret key, sample the link signature space in a physical area to collect and combine uncorrelated measurements channel based secrecy algorithms ,based on ITS key derivation protocol, in order to improve existing wireless security system had been laid down and modified as appropriate algorithms.
KEYWORDS*- authentication,,802.11i, physical layer, key, security, wireless.*

I. INTRODUCTION

The topic of privacy and security in wireless communication networks have taken on an increasingly vital role as these networks continue to spread worldwide. Security is viewed as an independent feature addressed above the physical layer.
Most of widely used cryptographic protocols are designed and implemented assuming the physical layer has already been established and provides an error-free link. However, with the emergence of adhoc and decentralized networks, higher-layer techniques ,such as encryption, are becoming difficult to implement.
Therefore, there has been a considerable attention paid on studying the inherent ability of the physical layer to provide secure wireless communications. This paradigm is, there for called wireless physical layer security. Physical layer security is an active research area that can achieve the possibility of finding perfect-secrecy data transmission ,while in the mean time , possibly malicious nodes that eavesdrop upon the transmission obtain none of information[2].
The fundamental concept behind wireless physical layer security is to exploit the characteristics of every wireless channel , and effect of such as fading or noise, to provide secrecy for wireless transmissions, While these characteristics have traditionally been seen as impairments. Physical layer security takes advantage of these characteristics for improving the security and reliability of wireless networks. Most of the focus of cross-layer optimization in wireless networks has been on enhancing basic network operations, such as routing and medium access control , and little attention has been devoted to using cross-layer information to enhance security[3] .

II. WIRELESS SECURITY MECHANISMS

Most of the focus of corss-layer optimization in wireless networks has been on enhancing basic network operations, such as routing and medium access control, and little attention has been devoted to using cross layer information to enhance security.

2-1 Threats and opportunities for enhancements

Securing network systems focuses on addressing confidentiality, dataintegrity, authentication ,and non-repudiation through protocol suites.
The main concerns of security design are as follows:
1-**Confidentiality**: the message and any part of it are kept secret from all but the legitimate sender and receiver, to have the right, to expose.
2-**Integrity**: the receiver is able to make sure that the message has not been modified during transmission and a false message cannot be substituted for a real one, Hence the system is integrable, but, with no modifications.
3-**Authentication**: the receiver should be able to verify the message origin, interrogator on process. This is fact of life, to be safe

4-**Non-repudiation**: the sender should not be able to deny having sent the message at a later time, because up on which, the data becomes vital, for right decision as the case of digital signature .
The first three have been of primary concern in the design of security systems, although non-repudiation is gaining importance, for example with the advent of applications for digital signatures[1].

2-3 Authentication Modes:

Among the innovations 802.1i is the introduction of two Authentication modes:
The first mode is based on the availability of an authenticationserver(hereafter referred to as 802.1x based authentication).

2-3-1First mode: 802.1x based authentication:

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server, as depicted in Fig.(1).
The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator[1].
The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAPprotocols[2]
.

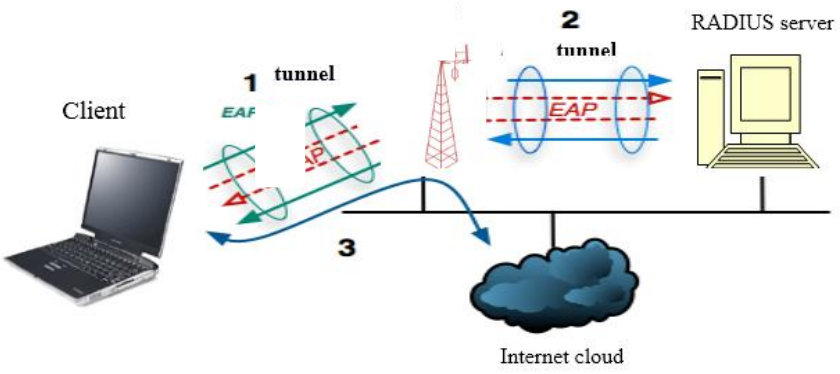


Figure (1) Authentication Using 802.1x

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration, before being allowed to enter the country[7].
With 802.1X port-based authentication, the supplicant provides credentials, such as (user name / password or digital certificate), to the authenticator, and the authenticator forwards the credentials to the authentication server for verification, process .
If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network[7].

2-3-1-1Key Components

802.1X relies on an integrated system of components to manage the authentication process:
1-**Supplicant**. Software or service running on a device that seeks access to a protected network, to share resources, it is client side.
2-**Authenticator**. Software or service running on a wireless access point or switch that manages the authentication process between the supplicantand 802.1x authentication server. It could work as intermediator.
3- Authentication server. Software or service that provides authenticationservices to the authenticator. Using the credentials provided by thesupplicant, the authentication server controls whether, the supplicant isauthorized to access the services provided on the authentication server'sprotected network.

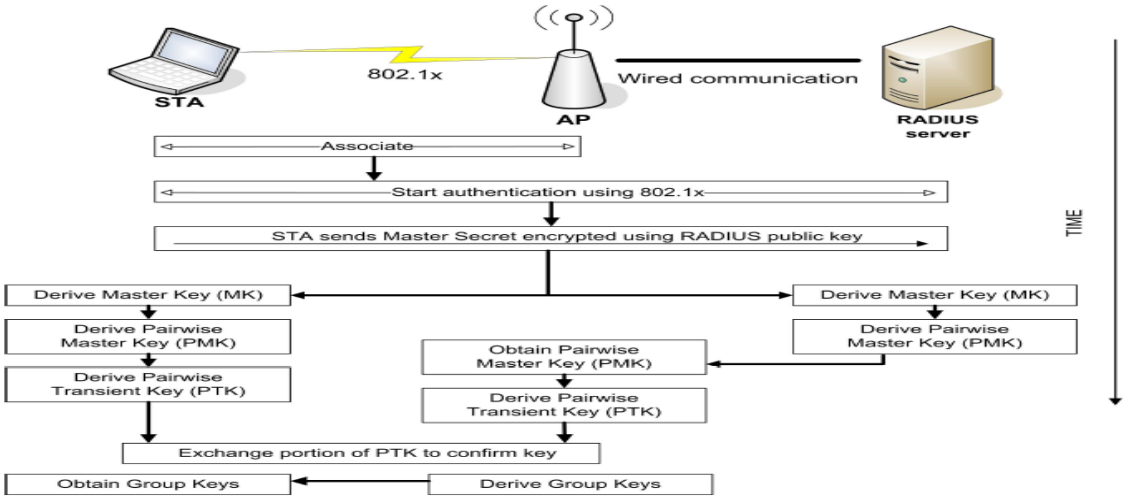
2-3-2 Second Mode:

It is based on configuring a secret password or pass-phrase on the participating devices: the pre-shared key(PSK) mode.
In the PSK mode a user authenticate by demon string knowledge of secret key. 802.1x basedauthentication is typically used in WLAN office or enterprise deployments.
It based on the availability of digital certificates at both the client as well as the authentication, authorization, andaccounting(AAA) server[1].

Fig.(2) summarizes the sequence of steps in the 802.1x authentication and key distribution process ,in the PSK mode association between the STA and AP replaces the communication prior to the establishment of the pair wise master key (PMK) in Fig.(3) .
The PSK then becomes the PMK, and the rest of the procedure is unchanged .Note that the master key(MK , shared by STA and AAA server) and PMK (shared by STA,AP and AAA sever) are not the same because the roles of the AP and AAA server are separated[2].
Further more ,the PMK and pairwise transient key(PTK) are not the same, since updating the entire mechanism is resource intensive ,the PTK is the key that is updated, as depicted in Fig.(4) [1].

2-4 Opportunities To Enhance 802.11i

Although 802.11i addresses wide range of security threats facing wireless LANs ,the protocol suite is not complete ,and there are many threats that can undermine 802.11i .
The research is filled with examples of exploits against 802.11i,ranging from denial of service(DoS) attacks to attacks that undermine 802.11i ,because it attempts to maintain backward compatibility[1] .
Although it may be possible to address such threats, through further refinement of the security protocol suite, many threats may easily be addressed in a cross-layer security framework, using information provided by the physical layer .
Spoofing attack on the identity of an access point (AP)(e.g.,the well-known deauthentication or disassociation attack),or by single client conducting a Sybil attack by claiming multiple network identities.Such a threat can be dealt with by tracking the channel responses an anomaly, indicating spoofing ,The physical layer also provides an opportunity to address risks associated with the compromise of the PMK in 802.11i[7].
In particular, by integrating secret bits extracted from the physical layer channel into the key establishment process, it is possible to achieve forward and backward secrecy[2].



Figure(2)Overview of 802.1x-based authentication and key distribution.

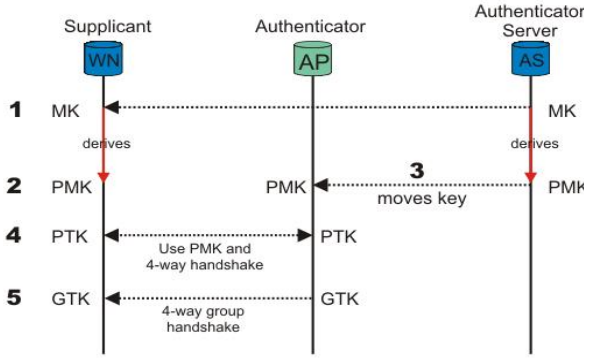


Figure (3) Key management and distribution in 802.11i.

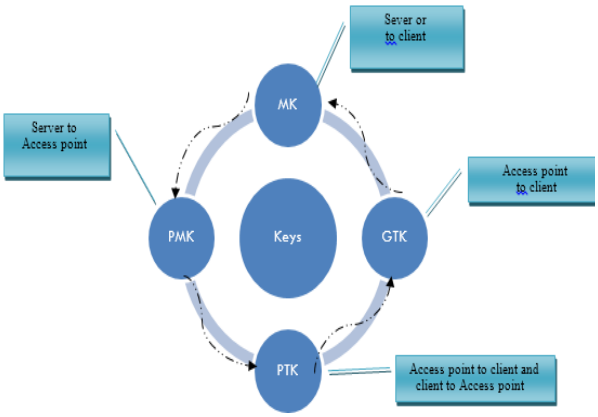


Figure (4) Keys rotation and their functions

III. ENHANCED CHANNEL–BASED SECRECY MODIFICATIONS

3-1Message-Digest (MD)

A message-digest algorithm is also called a hash function or a cryptographic hash function. It accepts a message as input and generates a fixed-length output, which is generally less than the length of the input message. The output is called a hash value, a fingerprint or a message digest.

MD5 is one in a series of message digest algorithms designed by Professor Ronald Rivest of MIT (Rivest, 1992). When analytic work indicated that MD5's predecessor MD4 was likely to be insecure, MD5 was designed in 1991 to be a secure replacement. (Weaknesses were indeed later found in MD4 by Hans Dobbertin) [10].

3-1-1 MD5 algorithm.

The main MD5 algorithm operates on a 128bit state, divided into four 32bit words, denoted A, B, C and D. These are initialized to certain fixed constants seeTable (1)these registers are initialized to the following values in hexadecimal, low-order bytes first. The main algorithm then operates on each 512bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages by equation (1) to equation(4) , termed rounds; each round is composed of 16 similar operations based on a non-linear function F, see equation(5), modular addition, and left rotation. Fig.(5) illustrates one operation within a round[6].

Table(1) fixed constants A,B,C and D

A	B	C	D
01 23 45 67	89 ab cd ef	fe dc ba 98	76 54 32 10

There are four possible functions; a different one is used in each round.

F(B,C,D)=(B AND C) OR(NOT(B)AND D) (1)

G (B,C,D) = (B AND C) OR (C AND NOT(D)) (2)

H(B,C,D)= B XORC XORD (3)

I(B,C,D)= C XOR(B OR NOT(D)) (4)

Each round has 16 steps of the form

$A \leftarrow B + ((A + F(B, C, D) + M[i] + K[i]) <<< s)$ (5)

$Ki=abs(\sin(1+i)) * 2^{32} \quad 0 \leq i<64$ (6)

Where; A, B, C, D: isrefer to the 4 words of the buffer, but used in varying permutations.
F: is a different nonlinear function in each round.
Mi: denotes a 32bit block of the message input.
Ki: denotes a 32bit constant, different for each operation.

: denotes a left bit rotation by s places.

:Denotes addition modulo 2^{32}.

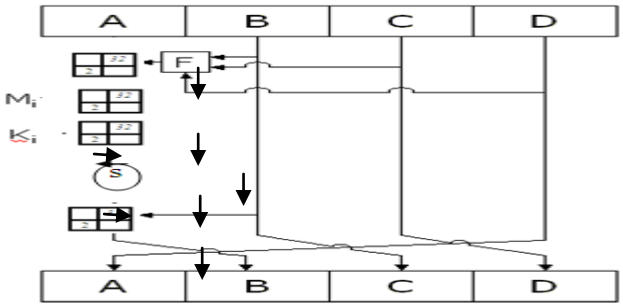
- **Implementation Steps**

In equation (5-6) uses a 64-element table k[0 ... 63] constructed from the sine equation ,denote the i^{th} element of the table, which is equal to the integer part of 2^{32}=4294967296 .Where i=0, k_0 **=(**D76AA478**)$_{16}$** to i=63, k_{63}=EB86D391.

The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations;

Round 1: Steps 0 thru 15, uses F function,see in equation (1).

Round 2: Steps 16 thru 31, uses G function, see in equation (2).
Round3: Steps 32 thru 47, uses H function, see in equation (3).
Round 4: Steps 48 thru 63, uses I function, see in equation (4).
Do the following 16 operations in Round 1.
Let [abcd k s i] denote the operation in equation (5).



Figure(5)Operation within MD5 realization .

3-2 **EnhancedChannel–Based Secrecy.**
The InformationTheoretic Secure (ITS) bits, may be used to improve existing wireless security systems.
Among the innovations of 802.11i is the introduction of two authentication modes. The first mode, is based on the availability of an authentication server (hereafter called 802.1x-based authentication). The second mode, is based on configuring a secret password or pass-phrase on the participating devices i.e. the Pre-Shared Key mode (PSK).
It should be noted that, with PSK mode, the implicit assumption is that a user authenticates by demonstrating knowledge of the secret key.
Although the existing 802.11i protocol features both very robust and secure, encryption algorithms, and an automated key distribution framework, it cannot address certain security threats intrinsic to conventional security design. In fact, one of the easiest ways to attack a secured system is to gain unauthorized access to the credentials of a legitimate user[2].
For example, suppose a malicious attacker is able to observe (or obtain knowledge of) the pass-phrase employed by a user when configuring his home WLAN or when accessing a public hotspot, the attacker will then have all the information he needs to break the encryption cipher of the legitimate user. Thus, the attacker may gain access to the WLAN and also eavesdrop on any traffic the legitimate user transmits[4].
To demonstrate how the introduction of ITS bits can improve the 802.11i protocol, we begin with minimal modification.

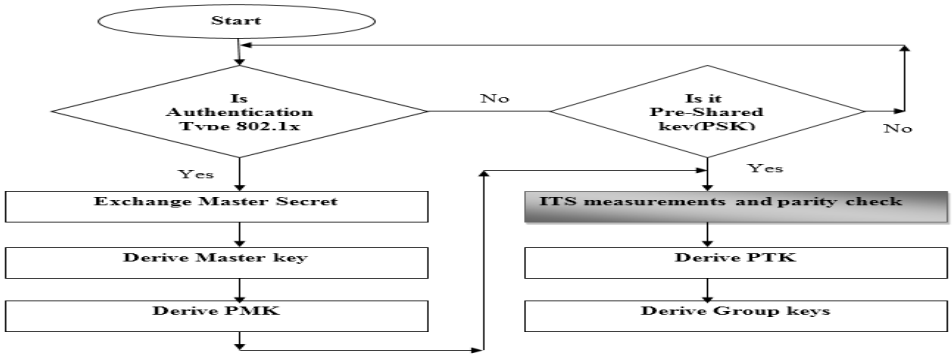


Figure (6) Using ITS in 802.11i Security

In Fig.(6) weshow how aWLAN transmission using PSK authentication mode can be modified using channel-based secrets.
In this approach, we simply use ITS stringsto derive the Pairwise Transient Key (PTK) from the PMK, PTK = Hash {PMK, PTK-old, Info in the clear, ITS bits},where the hash is a secure, one-way, many-to-one function. It is not only provides computational security for its input as a whole but makes sure that the presence of ITS bits makes it impossible to deduce PMK with acertainty that exceeds the entropy of the ITS bits.
The measurements required to generate the ITS bits can be carried out at any time prior to deriving the PTK .Likewise, the parity check exchange can also be carried out at any time prior to deriving the PTK.

Once the ITS bits and PMK are derived (in case of 802.1x) the PTK can be derived from the PMK using a pseudo-random function, The Group Key derivation and distribution can be left untouched. This is illustrated in modified flowchart in Fig.(6).
Having illustrated a simple way to make good use of the ITS bits available to us, we now depart from the key hierarchy in Fig.(7).
If 802.1 x authenticationsis used, the AAA server provides the STA its credentials.
The STA then verifies the AAA servers' credentials and provides its own credentials along with a secret. The AAA server then forwards the secret to the AP after verifying STA credentials. An Encryption Key (EK) is then derived by the STA and AP, using the secret and the ITS string. If authentication is PSK, then the Pre-Shared Key acts as the secret. Part of the EK is used for verification, while part of it, is used to protect group keys derived later. The remaining part is the portion actually used in the AES algorithm, We note that the key hierarchy in the proposed scheme is significantly simpler than the one in Fig.(7), In fact, the hierarchy no longer exists. Instead, we simply have the following two sets of keys:
• The Pre-Shared Secret used for authentication.
• An intermittently updated Encryption Key which is used for actual data transmission.
Let us examine how the proposed scheme addresses the security threats we discussed above. Suppose that an eavesdropping terminal has been able to gain access to a user's PSK and is eavesdropping on the transmission, the eavesdropper is able to obtain the PMK – but can go no further, Unless the eavesdropper is physically co-located with either the AP or the terminal, it cannot obtain the ITS bits used to derive the PTK[4].
Similarly, the scheme in Fig.(7) permits the eavesdropper to realize that authentication has transpired, but does not allow eavesdropping on actual data being transmitted With the scheme in Fig.(8).

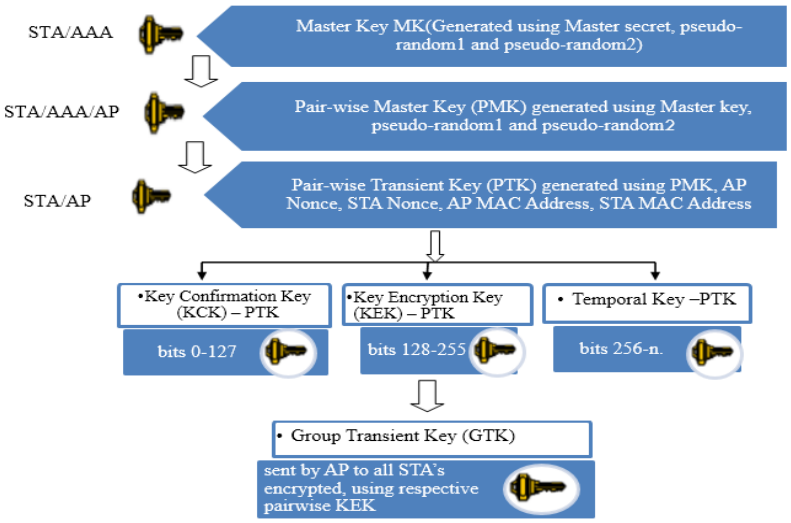


Figure (7) 802.11i Security Key Hierarchy

Note also that the proposed scheme provides specific forward and backward security. Since ITS strings are constantly generated (we have a positive ITS rate over time), this fresh set of ITS bits can then be immediately used to derive a new PTK or a new EK for communication. Since the terminals involved generate the ITS bits in sync, the process is naturally synchronous. Forward and backward secrecy versus information transmitted with previous PTK/EK is immediately achieved: even if an eavesdropper obtains the current PTK/EK, it is statistically uncorrelated to previous or to future ones, and therefore the eavesdropper is unable in principle to learn those keys. Thus, even when the key is completely exposed, data is vulnerable only during the period of time it takes to accumulate enough ITS bits for a new key[2].
A simple modification of the protocols presented prevents the attacker from being able to work back towards the PSK - even if the attacker obtains a particular set of ITS bits. The required change is simply do not use the PSK in the derivation of the PTK/EK. The gain here is a complete separation of the authentication procedures from the data encryption processes.

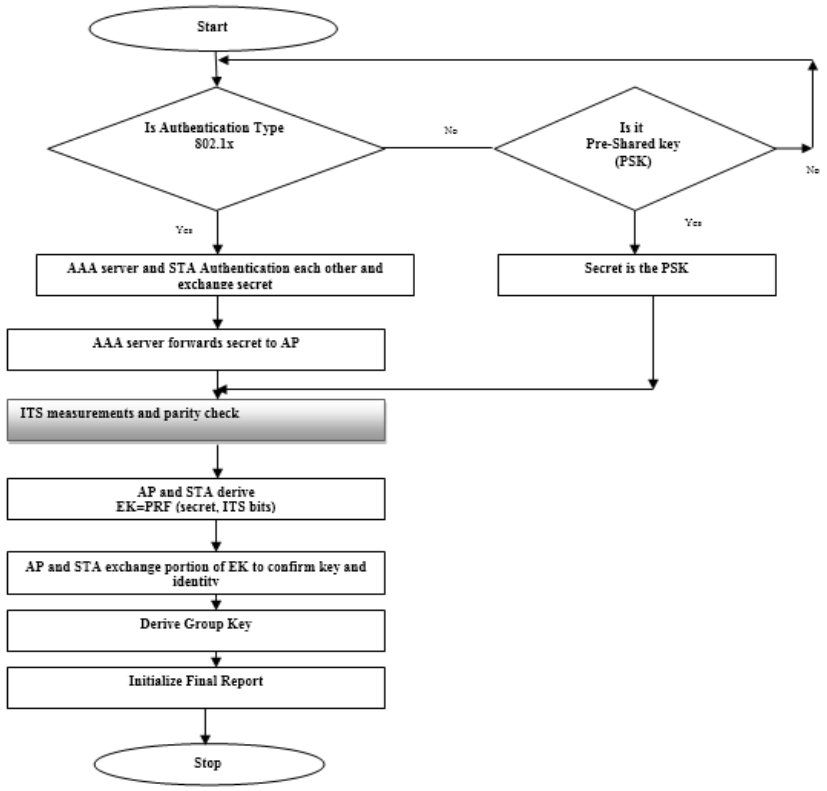


Figure (8) New 802.11i key Derivation Protocol

Now that we have considered how this source of physical layer information may be used to improve existing wireless security, let us consider what other uses this information may be put to use.
A general weakness of wireless security is Denial of Service (DoS) attacks[5].
For example consider a scenario where the MAC layer is receiving correctly received packets from the physical layer. However, the rate of reception is somewhat lower than the apparent physical channel capacity. At the MAC layer it is difficult to separate this problem between that of a subtle DoS attack or genuine poor channel quality. However, recall that the original premise of the ITS security is that the channel observations between two nodes communicating, with each other are mutually unique and significantly different from a third eavesdropping node as long as that node is at least half a wavelength away. This characteristic enables the terminals to in essence consider the CIR as a finger-print of the transmitter from which the signal is emanating. In essence using the physical layer information at our disposal, we are able to continuously authenticate packets at the physical layer.This form of security is only possible through physical layer security mechanisms[8].

IV. SIMULATION RESULTS OF SECURITY IN PHYSICAL LAYER

4-1 Enhanced Channel–Based Secrecy Results

In the simulation environment, generated keys PMK and PTK by MK,Info in the clear and ITS bits. For more detail see Fig.(9).
In which, ITS can be measured, where the (PTK), can be derived, using ITS string , and PTK, is also equal to the Pseudo-Random- function, with attributes (PMK, Info, ITS bits).
Hash result is also obtained, in order to obtain , one –way massage digest, for, MK added to Pseudo-Random , for every run. Column table of ITS string, PTK,PMK, and MAC address are given.

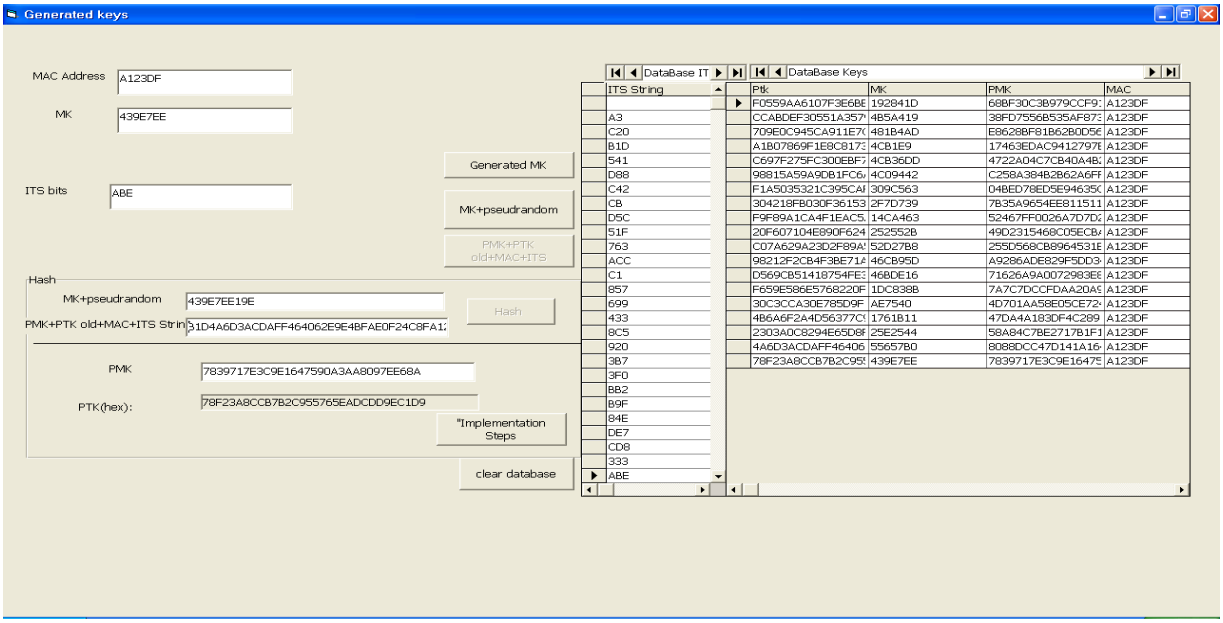


Figure (9) Generated Keys

4-1-1Generated ITS bits (Nonce)

A nonce is an arbitrary number used, only once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number, issued in an authentication protocol to ensure that old communications cannot be reused, in replay attacks.Therefore, to ensure that a nonce is used only once, it should be time-variant (including a suitably fine-grained timestamp in its value) see in Fig.(9) and Fig.(10),However, after generated ITS bits just store values in database , for the sake of the parity check exchange can also be carried out, at any time prior to store in database. For more detail see Fig.(11).

.4-1-2 Derive Pair-wise Transient Key (PTK)

Generated Pair-wise Transient Key(PTK) using a message-digest algorithm is also called a hash function .This can be illustrated in Fig.(9).Pair-wise Master key (PMK) generated, using Master key and pseudo-random . *PMK=hash{MK, pseudo-random} ,PTK = Hash{PMK, PTK-old, MAC Address, ITS bits}.* This can be illustrated in Fig.(12).

4-1-2-1 Hashing Function Cryptosystem

A hash function $h = H(m)$ takes a message $'m'$of arbitrary length as input and produces a fixed-length bit string $'h'$as output, it is computationally infeasible to find the input 'm' that corresponds to a known output $'h'$.

Figure (10) Generated ITS bits(Nonce)

The weak collision resistance property, given $'m'$ and $h = H(m)$,it is computationally infeasible to find another m',($m' \neq m$), such that $H(m) = H(m')$,the strong collision resistance property, when only given H, it is computationally infeasible to find two different m and m'.This can be illustrated in figFig.(13).

The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations see Fig.(11);

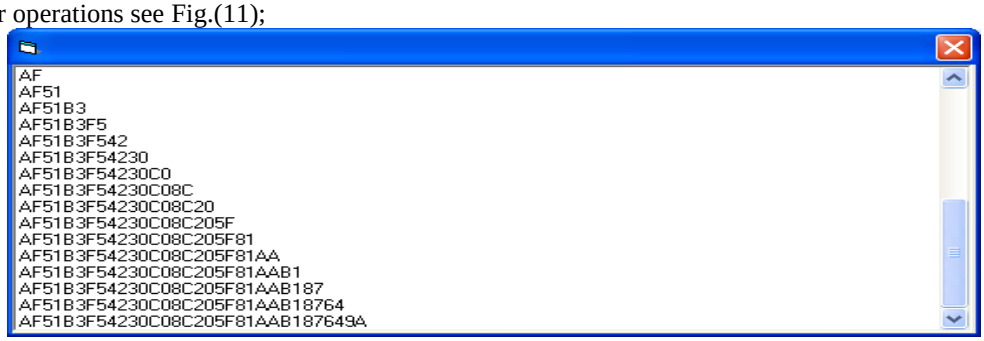


Figure (11) Results Implementation Steps

4-1-2-2 Result system

Table(2) Show, results generated keys PMK ,PTK and ITS bits, Since keys PMK and PTK are each of size 128 bits, and size ITS bits are changed.If the eavesdropper is able to obtain the PMK, but can go no further sinceit cannot obtain the ITS bits used to derive the PTK. If for eavesdropper to realize that authentication has transpired, but will not allow it to eavesdrop on actual data being transmitted.Since ITS bit-strings are constantly generated in time, we are regularly provided with a fresh set of ITS bits, that can then be immediately used to derive a new PTK or a new EK for communication. The following results;

Table(2)Result system (PTK,PMK,ITS bits)

PTK	PMK	ITS bits
F0559AA6107F3E6BE5585AD76DEFBB2C	68BF30C3B979CCF91CE6185029E15279	5317
CCABDEF30551A3579C37842A5395D6D0	38FD7556B535AF873FFCC17360ACAB88	1B3D
709E0C945CA911E7C0677DD1D41532FC	E8628BF81B62B0D56E89622E66B47FC8	4C8E
A1B07869F1E8C81734F8925071CE99AD	17463EDAC9412797E1F7BDC01DA19AD0	A98
C697F275FC300EBF74D2B2308316BF6E	4722A04C7CB40A4B2F86721B306A3639	6BB
98815A59A9DB1FC6AA7D813278241923	C258A384B2B62A6FF20B05215E7E93E3	224D
F1A5035321C395CAF3795F19B6841016	04BED78ED5E94635CC3A4E874ED22B3D	670D
304218FB030F36153C81D6A7B99C8F00	7B35A9654EE811511B0C205D6B66513A	2604
F9F89A1CA4F1EAC5A415F13E59E826EA	52467FF0026A7D7D2D0AB7B7039C650E	78A9
20F607104E890F624B1AB565A3A04B0A	49D2315468C05ECBA2843322A662C35D	59D
C07A629A23D2F89A57951877B4A2A101	255D568CB8964531BB21744876431461	383C
98212F2CB4F3BE71A09892D7FC151C2E	A9286ADE829F5DD3445698A091CD7C79	CDC
D569CB51418754FE3ECF4B33886DC94A	71626A9A0072983E8D6D7E6EEC5C48F5	5B27
F659E586E5768220F58900221389B6C2	7A7C7DCCFDAA20A921F092109F8BA8F8	77EE
30C3CCA30E785D9F1E366FD3FC8C2A5F	4D701AA58E05CE724FE47D10D0BD289B	6D93
4B6A6F2A4D56377C954E9BE0E21DA618	47DA4A183DF4C2891E0C25AD42648500	4752
2303A0C8294E65D8F8D96F76BB3D4679	58A84C7BE2717B1F11D586D1904DAF5C	7841
4A6D3ACDAFF464062E9E4BFAE0F24C8F	8088DCC47D141A164FD3942C0BF975DA	387A
78F23A8CCB7B2C955765EADCDD9EC1D9	7839717E3C9E1647590A3AA8097EE68A	58FD

- **Result;**

If MAC address = A123DF , MK =4B5A419, MK+ pseudo-random = 4B5A41982

PMK =Hash (MK+ pseudo-random)=38FD7556B535AF873FFCC17360ACAB88 , ITS bits = 59D, Then

PMK +ITS bits +PTK old + MAC address =
38FD7556B535AF873FFCC17360ACAB8859DF0559AA6107F3E6BE5585AD76DEFBB2CA123DF

PTK= Hash(PMK +ITS bits +PTK old + MAC address) = CCABDEF30551A3579C37842A5395D6D0

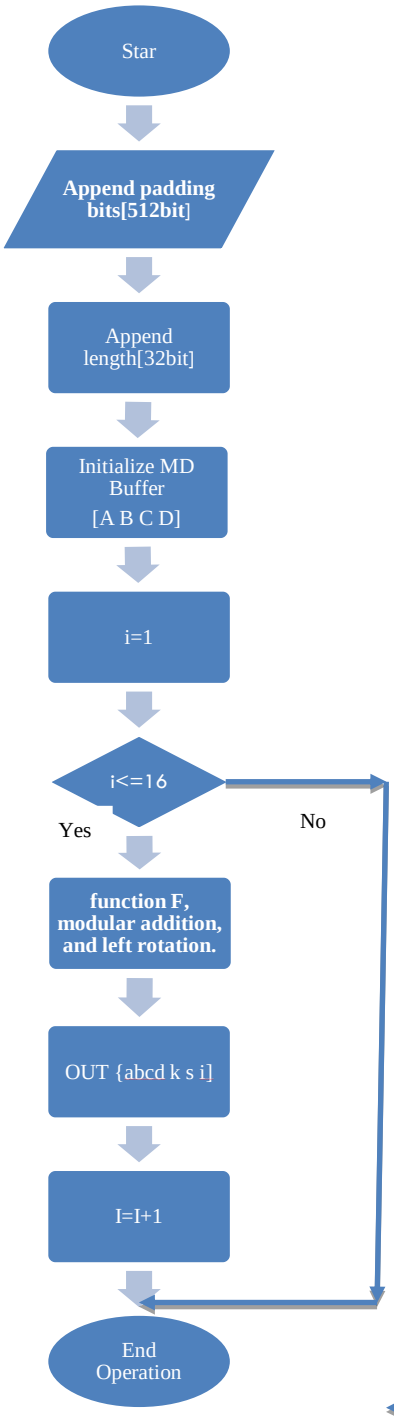


Figure (12) Hashing Function

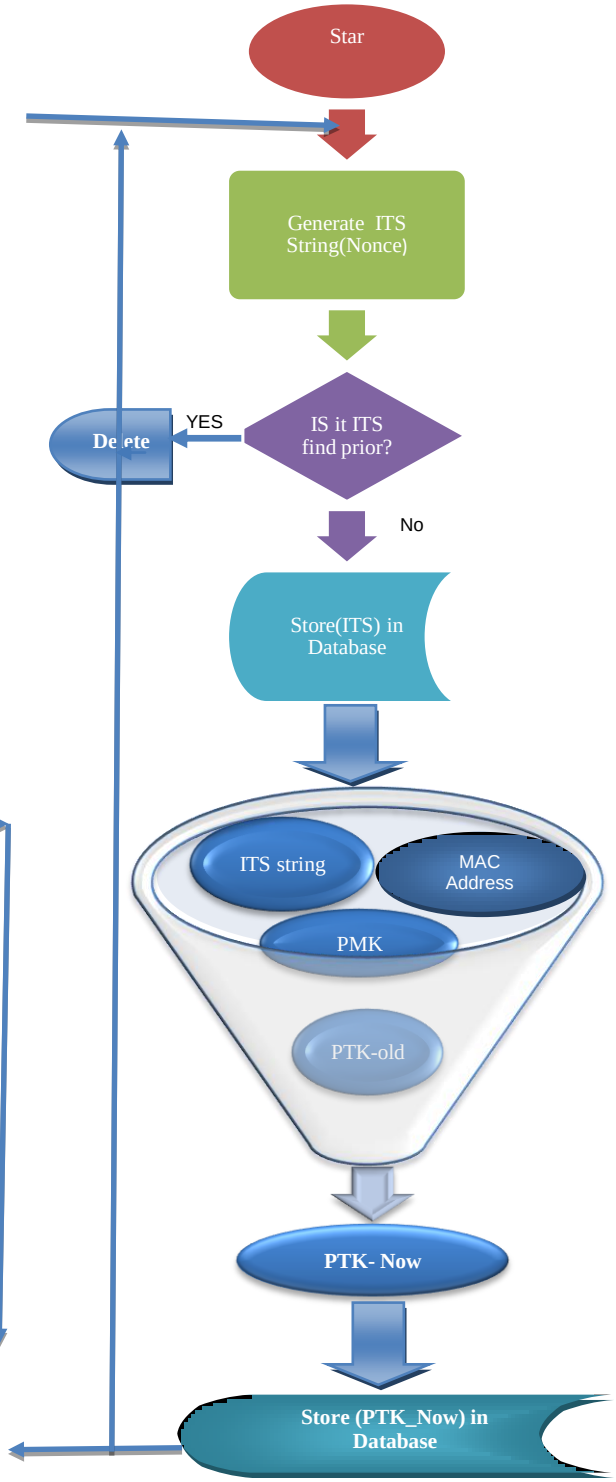


Figure (13) Generated Pair-wise Transient Key(PTK)

Since ITS bit-strings are constantly generated in time, we are regularly provided with a fresh set of ITS bits that can then be immediately used to derive a new PTK or a new EK for communication. Finally, we note that attacks where Eve impersonates Alice in the key extraction protocol can be dealt with using physical layer authentication, in a manner similar to that in [3], [10].

Furthermore, the fact that the channel follows reciprocity allows thecollection of highly correlated information, which canbe used to extract a string of secret bits for use ascryptographic keying material. Thereby, the channel alsoprovides a simple means for enhancing confidentialityservices in wireless networks.

V. CONCLUSION

The selectivity and uniqueness of a wireless channel,along with the fact that the channel decorrelates away in space over distances, that are on the order of wavelength ,can allow the channel to be used as a means, to prevent spoofing attacks and thus maintain an authenticator for the legitimate transmitter,dealt with enhanced channel-based secrecy, in terms of using ITS in 802.11i security and key derivation procedure, their basic flowcharts were introduced.We have demonstrated how wireless channel reciprocity may be used to extract secret keys; and how these, in turn, may be used to enhance the existing 802.11i protocol.

VI. ACKNOWLEDGMENTS

We would like to thank the editors and the anonymous referees whose insightful comments helped us toimprove the presentation of the paper.

REFRENCES

[1] S.Mathur et al.,*radio –telepathy:extracting a cryptographic key from an unauthenticated wireless channel*(14th ACM Mobicom,2008).
[2] Mather,Suhas,*exploiting the physical layer for enhanced security*(Rutgers University,October2010).
[3] Matthieu Bloch, Student Member, *wireless information-theoretic security*(6th, JUNE 2008).
[4] Alex Reznik, Yogendra Shah, *enhancing wireless system security with phy-Layer technique(*Inc 781 Third Ave King of Prussia, PA 19406, USA).
[5] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, *fingerprints in the ether: using the physical layer for wireless authentication*,(Proc. ICC 2007).
[6] Harley Kozushko, The message-digest algorithm MD5,2003.
[7] "802.1X Port-Based Authentication Concepts"http://www. wireless-nets.com/resources/downloads/802.1x_C2.html. Retrieved 2008-07-30
[8] L. Xiao et al , Using the Physical Layer for Wireless Authentication in Time-Variant Channels , IEEE Trans .Wireless commun. , 2008.
[9] Apple Technical White Paper, 802.1X Authentication, OS X 10.7.3 and iOS 5.1, May 25, 2012.
[10] Michael Raggo, Wireless Insights , Wireless Security , http://www.net-security.org/secworld.php, January 2010.