# A Multi-Key Encryption Scheme for the Next Generation Wireless Network

Chia-Chen Hung Eric Hsiaokuang Wu* Cheng-Lin Wu Ruei-Liang Gau Yi-Cyuan Chen

Department of Computer Science and Information Engineering

National Central University

Chung-Li 320, Taiwan, ROC

{cory, Hsiao, graffine, gary, emn178}@wmlab.csie.ncu.edu.tw

*Received 16 November 2007; Revised 30 November 2007; Accepted 9 December 2007*

**Abstract.** The fast growth of Internet technology has suggested that the next Generation Wireless Network (NGWN) will be an all-IP based integrated wireless network architecture. This evolving network will realize a great number of novel mobile network applications and innovated ubiquitous computing services. As more and more emerging interactive service developments proceed within the wireless network, the security of confidential data and individual privacy become a critical issue. Current wireless security technologies have faced potential challenges; thus they might not be able to satisfy some special requirements of NGWN. We have been devoted to a long term research project to provide solutions to meet the requirements of mobility and security for NGWN. This paper is demonstrating our first stage research accomplishment, a novel wireless security mechanism called Multi-Key Encryption (MKE) mechanism. This mechanism enhances the key management of Wi-Fi Protected Access 2 (WPA2), which has a strong robustness and the similar computation overhead. Through the formal proof and experimentation result, we can show that our mechanism is effective and able to provide necessary security. In the future, we will continue to extend it to generic security solutions for NGWN.

**Keywords:** next generation wireless network**,** wireless security**,** 802.11i, key management, multi-key encryption

## 1 Introduction

In recent years, the fast-developing Internet network has begun to have a great effect on human's life [1, 2]. Through the progress of wireless network and popularization of mobile devices, people can access data or complete business transactions at any time and anywhere. In addition, the successful combination of wireless communication and electronic commerce further prompts the e-commerce trend to become portable and ubiquitous. As more and more activities proceed within the Internet, communications through network are not only data, but also multimedia information. At the turn of the last century, telecommunications objective changed considerably, for example, from traditional wired telephony-oriented services to data-based services, from unintelligent machines to digital assistants and mobile computers, and from homogeneous networks to heterogeneous networks. It has been evolving to construct an IP-based next generation network (NGN).

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) had defined NGN [3]: NGN is an integrated network based on packet transmission. It can supply current telecommunications services and offer efficient wideband transmission capability and appropriate quality of service (QoS) guarantee. In this service platform, services will not be constrained by transmission technologies. Users are free to connect to NGN without limitations and select different telecommunication provider and services. Driven by Internet technology, it is highly desirable to offer adaptive multimedia services via different wireless technologies (such as WLAN, WiMAX, WPAN) and distinct network architecture (such as cellular infrastructure, or mesh network). This great combination of the growth of the Internet and the wide deployment of wireless technologies will revolute a great number of new generation mobile applications and context-aware ubiquitous services. We refer to this integrated network as the Next Generation Wireless Networks (NGWN).

NGWN carries several key criteria:

- *Mobility management*. For worldwide networked environment, NGWN must provide automatic roaming.
- *IP transparency.* All elements both in the fixed and mobile parts of the network must support IP.
- *Addressing*. NGWN must allocate an absolute address to each user. IPv6 will be adopted in the future.
- *Integrated digital services.* Supporting broad services, applications, and frameworks, which including

* Correspondence author

real-time video streaming, non-real time services, and multimedia services.
- *Transmission*. Capabilities for wideband and end-to-end QoS transmissions.
- *Security and digital rights management*. NGWN must be fit in with all kinds of security rules such as privacy, integrity, and so on.

The vision of NGWN can be realized over various wireless networking access technologies such as Bluetooth, Wireless Fidelity (Wi-Fi), Worldwide Interoperability for Microwave Access (WiMAX), and High Speed Packet Access/Universal Mobile Telecommunications System (HSPA/UMTS). Apart from innovations in network technologies and mobile applications, the security of confidential data and individual privacy will become a critical issue.

Security goals for wireless networks can be summarized as follows. Message authentication provides integrity of the message authentication, corresponding to the attacks of message modification. Confidentiality and privacy is fundamental for secure communication, which provides resistance to interception and eavesdropping. Access control prevents unauthorized access. Anti-replay detects and neglects any message that is a replay of a previous message. Non-repudiation is against denial and pretense. Detailed discussion of the security requirements, together with corresponding attacks and possible solutions, can be found in [4] and [5].

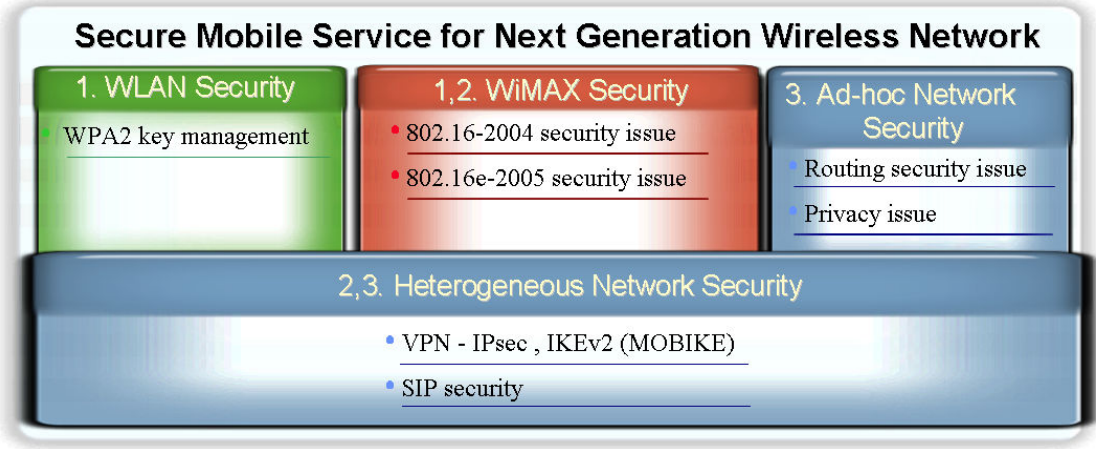


**Fig. 1.** SMS-NGWN architecture

To provide and satisfy the requirements of mobility and security for NGWN, a three years project, named Secure Mobile Service for Next Generation Wireless Network (SMS-NGWN), is proposed and shown as Fig.1. In first stage, we attempt to solve key management issues of current wireless local area network (such as Wi-Fi) security mechanisms. Besides, we also survey the network structure and security mechanism of wireless metropolitan area network (such as WiMAX). The second year, we will transplant first year's achievements to WiMAX network. In addition, we intend to propose a generic security solution, which could be constructed on virtual private network (VPN) [6], to heterogeneous networks for NGWN. Finally, we will also extend the security function over ad hoc network and integrates the three stages for NGWN.

In this paper, we focus on the first stage of our project. Section 2 introduces common wireless security attacks and current security mechanisms of Wi-Fi and WiMAX. In Section 3, we proposed a key management scheme to enhance Wi-Fi security. In Section 4 and Section 5, we validate our scheme through formal proof and experimentation. Section 6 concludes this paper and talks about our future work.

## 2 Related Work

### 2.1 Common Wireless Security Attacks

The traditional attack modes in wireless network can roughly be divided into two parts: passive attack and active attack [7].

A passive attack is one in which the cryptanalysis can't interact with any modification involved, attempting to break the system solely based upon observed data. The common approaches of passive attack are Eavesdropping and Traffic Analysis. The Eavesdropping is to surreptitiously overhear a private conversation. Traffic Analysis is

the process of intercepting and monitoring in order to deduce information from flows, contents, and behaviors in communication. Both they can be performed even when the messages are encrypted and cannot be decrypted.

Contrast to passive attack, active attack means attack forges or modifies the communication contents. It can operate by Man-in-the-Middle (MITM), Replay, Denial of Service (DoS), and Dictionary. In MITM, an attacker is able to read, insert, and modify messages between two parties by observing and intercepting messages between the two preys. A replay attack intends a valid data transmission is fraudulently repeated or maliciously, so adversary can masquerade a legitimate user to illegally access system resources. Message modification implies that aggressor inserts, deletes, or modifies transmission data. The goal of a DoS attack is to retransmit a lot of useless packets in a few times to deny legitimate users to access to a resource by breaking down the resource itself.

A dictionary attack is a technique that trying to crack the decryption key or passphrase by searching a large number of words. It only tries possibilities typically derived from a list of words in a dictionary.

As the wireless network develops, some burgeoning attack activities were spring up, too. War driving [8] means that using certain mobile device, such as Laptop or PDA, to search usable Access Point (AP) nearby. Attacker hides in the car and drives everywhere, and nobody can be aware of that. Some attackers think that war driving is one kind of activity. Even they share the result which they searched everywhere on the web. Although there are developed some secure mechanisms, such as WEP, WPA and WPA2, some weaknesses and attacks were discovered, too. Some people say they only want to access internet, and some people say they do this just for fun. However, it implies problems of wireless network. It is a simple action to search AP from the beginning, and it developed methods of attack later. Nowadays, we call all actions of attack in wireless network to "War driving".

The other newly risen way is Evil Twin [9]. Evil Twin is a term for a rogue Wi-Fi AP that appears to be a legitimate station provided on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications. An attacker may use Evil Twin Attack to steal the passwords of unaware users by either phishing or snoop the communication, which setting up a crooked Web site and enticing people there. A rogue Wi-Fi connection can be built up on a laptop with a simple program and a special Universal Serial Bus (USB) drive that acts as an AP. The APs are hard to seek, since they can immediately be shut off, and are easy to set up. An attacker can appear to be legal by simply making their AP a similar name to the Wi-Fi network on the premises. Because of the attacker may be physically closer to the dupes than the real AP, their signal will be stronger. The attacker also can be configured to pass the person through to the true AP while monitoring the traffic of communication. Attackers typically build up Evil twin attacks near free hotspots, such as cafes or airports.

While most classical ciphers are vulnerable to this form of attack, the most modern ciphers should be designed to prevent this type of attack above all others.

### 2.2 Overview of Wi-Fi Security

Wi-Fi networks adopted as a framework for wireless local area network (WLAN). It based on IEEE 802.11b/g standards and has become popular in recent years. Many users have installed Wi-Fi AP at home, and numerous enterprises have already constructed WLAN environment. The individuals are easier to access services and public data through wireless network.

Since the wireless environment is a shared media networks, the transmitted messages can be intercepted easily. Therefore, it is important to protect the privacy of the transmitted data over the wireless environment. There are three major security components (authentication, integrity, and privacy) defined by IEEE 802.11 [10].The authentication has been divided into two parts: Open System and Shared Key. The main purpose of authentication services is to verify the legitimacy of a user or a system. The integrity protects the data against non-authorized insertions, modifications, or deletions. The privacy service guards the data against non-authorized revelations. In 802.11, the privacy service is implemented by the Wired Equivalent Privacy (WEP) protocol which is based on the RC4 symmetric algorithm. Several vulnerabilities of WEP protocol have be analyzed and discovered in the last few years [11, 12, 13]. In order to keep key changing ceaselessly, WEP uses a 64-bits key long, formed by an Initialization Vector (IV, 24bits) and a secret key (40bits).

One of WEP's security problems is that its secret key is not longer enough. The other problem is the initialization vector (IV) was sent to receiver in plaintext, which means that attackers can directly snatch IV of each key used in WEP. The same IV might be reused after short period of time. An attacker could easily collect IV and use it to retrieve the secret key. Besides, WEP also suffers from a poor method for key management, which adopts unchanged keys for long periods of time.

In order to improve the secure defects of 802.11, IEEE proposed a new amendment to IEEE 802.11 named IEEE 802.11i [14]. It defined a protocol that uses the Temporal Key Integrity Protocol (TKIP) as a short-term solution as well as Wi-Fi Protected Access (WPA) [15, 16]. The Wi-Fi Alliance created the WPA standard, which defines security mechanisms for authentication, data integrity, message privacy, and key distribution in Wi-Fi networks. Suitable to residence as well as enterprise users, it is designed to run on existing hardware as a

software promote and is compatible with the new IEEE 802.11i standard.

To improve message protection, WPA adopts the TKIP, which is designed to position all known attacks against and drawbacks in WEP algorithm. TKIP defends against perceives message modification, replay and brute-force attacks, and averts key reusing. In the long term, 802.11i might provide a framework which adopts the Advanced Encryption Standard (AES) [17].

For authentication solution, WPA implements the IEEE 802.1X standard for port-based access control [18] and the Extensible Authentication Protocol (EAP) [19]. 802.1X is now widely deployed in many IEEE 802 series standards with the RADIUS (Remote Authentication Dial-in User Service) [20], a central authentication server, to authenticate each user on the network. RADIUS could provide authentication, authorization, and accounting (AAA) services, but it still can't solve all security threats in wireless networks. Therefore, Diameter [21] is developing to improve RADIUS to supply more security.

EAP is a transport protocol fitted to the demands of upper-layer authentication protocols. It provides a plug-in structure for numerous popular upper layer application (ULA) protocols using today [22]. These protocols generate keys for data encryption on wireless transmission between AP and mobile stations. They are also in support of a mutual authentication exchange between the Radius server and a mobile station locating on the network. For small office/home office (SOHO) environment, where there is no EAP framework or central authentication server, WPA operates in a pre-shared key (PSK) mode, for which a user must enter passwords before join the network.

In pre-shared key mode, the passphrase may be stored both on the user's computer and Wi-Fi AP. However, the weak passphrases which users typical adopt are vulnerable to password cracking attacks (also called dictionary attack). A straightforward formula, proposed from [23, 24], that would reveal the passphrase by performing a dictionary attack against WPA-PSK networks. By capturing the 4-way authentication handshake, the attacker can have the essential data which needed to subject the passphrase to dictionary attack. Some WPA cracker tools [25, 26] have released. They are written on Linux systems and perform a brute-force dictionary attack against WPA-PSK networks. The users only have to supply a dictionary file and a dump file that contains the WPA-PSK four-way handshake.

Another attack way is DoS attack [27]. For example, an attacker could generate numerous connection requests to a server, effectively blocking this server for a long time. Because of Wi-Fi networks lack of encryption and integrity protection even when WPA or 802.11i is utilized, an attacker can easily forge management packets and send unauthorized packets or disassociation packets to the mobile station or AP, thereby denying legal packets. Radio-frequency-based DoS attacks at a Wi-Fi network's physical layer are also possible. There are no efficient countermeasures against DoS attacks [22].

### 2.3 Overview of WiMAX Security

WiMAX is a framework, proposed by the WiMAX forum, based on the IEEE 802.16 standard. IEEE Standard 802.16-2001 [28], completed in October 2001, promises to deliver high data rates (75Mbps) over wide areas (50Km) for a large number of users. The IEEE 802.16-2004 standard [29] aims to provide broadband wireless access for Wireless Metropolitan Area Networks (WMAN) and the recently released IEEE 802.16e [30] supports mobility and multicasting. Multicast in WMAN is a guaranteeing service, which suitable for many applications such as pay per view TV broadcasting, stock option bidding, video conferencing, and etc, for both fixed and mobile subscriber stations.

[31] gives a technical overview of 802.16. There are also some other papers or books that review this standard. It is clear that so far WMAN has been less studied than WLAN. With its great potential in the future's wireless service, WMAN deserves more attention than what it gets now. The authors of [32] review the 802.16 standard, and analyze its security in many aspects, such as vulnerability in authentication, data encryption algorithm, key management protocols, and lack of explicit definition for some materials. In [33], the architecture for point-to-point (PMP) mode was given too.

Mutual authentication is the major contribution proposed by [32], which enables SS to authenticate BS as well. Although the need for mutual authentication has been widely studied in WLAN, the authentication and key management protocols in 802.11 and 802.16 are based on different methods. IEEE 802.11 applies the shared-key authentication method, but IEEE 802.16 is based on public-key authentication algorithm. Therefore, the authentication and key management scheme in IEEE 802.16 needs separate study. In the standard IEEE 802.16e, mobility is supported in WMAN. The author of [34] gives an overview of handoff schemes on different kinds of networks and proposes the requirements for handoff procedures in IEEE 802.16. Due to the limited capability of wireless devices, such as power, storage, and computation ability, it is important to reduce the computation overhead for encryption or decryption. The authentication scheme of fast handover is based on EAP, which is implemented in IEEE 802.16 PKMv2 [35].

[36] gives comments on modifying some keying materials which should be exchanged during the roaming. Several types of attacks mentioned before, such as replay attack and interception, are also applicable to this protocol.

### 2.4 Summary

Nowadays, more and more products adopted wireless technologies (such as WLAN and WMAN), as the basic equipment, the security issues on wireless network become more important, too. From above mentioned, we can conclude that wireless security still suffer some attacks like War Driving and Evil Twin. Both WLAN and WMAN still have some security problems such as authentication, key management, message integrity, and so on. In this paper, we proposed a key management scheme called multi-key encryption (MKE) for dictionary attack to enhance existing Wi-Fi security system. In the future, we will extend it to WiMAX network and to propose a generic security solution for NGWN.

## 3 Multi-Key Encryption Mechanism

In WPA and WAP2 protocol, 4-way handshake performs the key management role as refreshing the temporal key for data encryption. As the original design, there exists a vulnerability in 4-way handshake stage, some attacking tools such as Aircrack [37] can crack the PMK key using dictionary attack. Hence, we modified the key management state in WPA as Fig. 2. The detail of the original 4-way handshake in 802.11i is as Fig. 3.

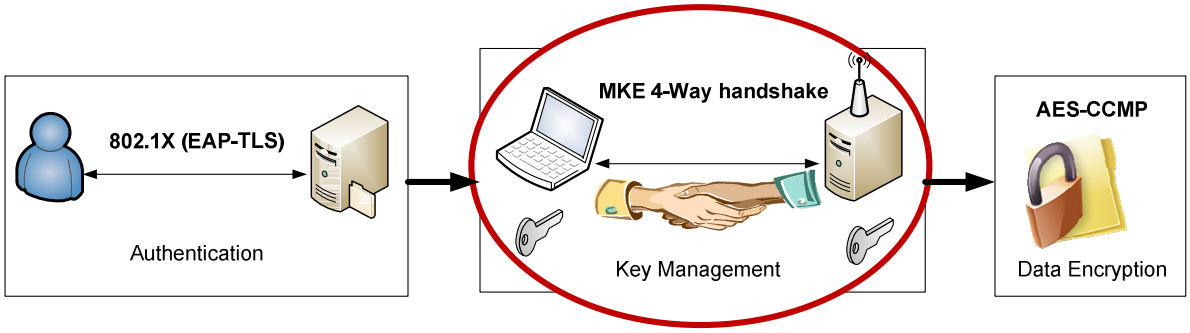


**Fig. 2.** MKE Encryption procedure

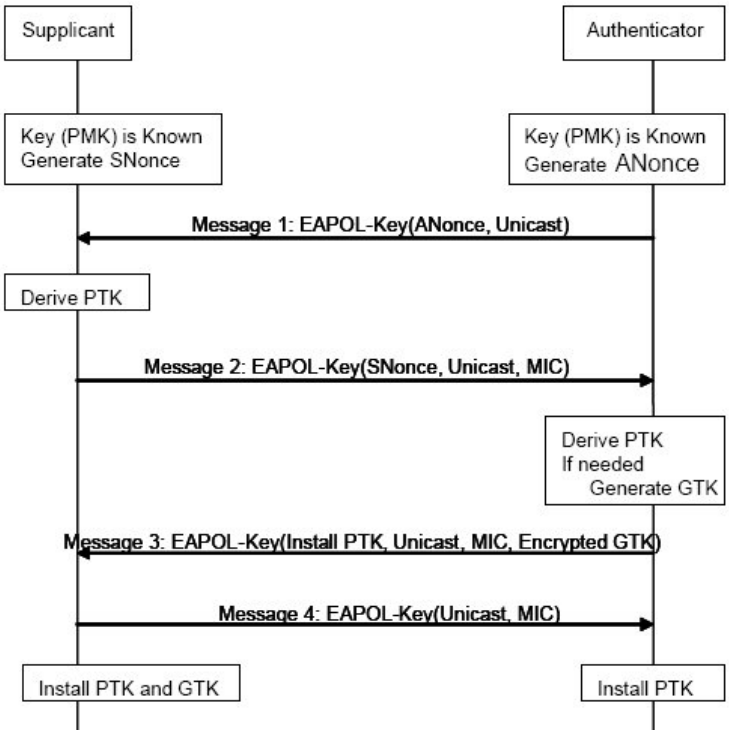


**Fig. 3.** 4-way handshake defined in 802.11i

Obviously, ANonce, SNonce and MIC transmit in plaintext. We recall that PTK is generated by the PRF-384 hash function as follows:

$$\text{PTK} = \text{PRF-384 (ANonce, SNonce, PMK, } MAC_{Auth}, MAC_{Supplicant}) \quad (1)$$

It's easy to get the $MAC_{Auth}$ and $MAC_{Supplicant}$ from packet header; hence, the only unknown value is PTK. However, the integrated check value MIC is generated from PTK using HMAC-MD5 or HMAC-SHA1-128 hash function and transmit in plaintext either. Therefore, the attacker can apply dictionary attack against PMK and verify the MIC to confirm the guessing.

### 3.1 Multi-Key Encryption (MKE)

Due to this vulnerability, we proposed the Multi-Key Encryption (MKE) mechanism to enhance the key management state in 802.11i. We introduce another SPK (second pre-share key) which installed on both authenticator and supplicants and the length is 32 byte just like PMK. The procedure of constructing PTK is modified as Equation (2), (3) (which DSK is stands for Derived Second pre-share Key):

$$\text{DSK} = \text{PRF-256 (ANonce, SPK, } MAC_{Auth}, MAC_{Supplicant}) \quad (2)$$

$$\text{PTK} = \text{PRF-384 (DSK, SNonce, PMK, } MAC_{Auth}, MAC_{Supplicant}) \quad (3)$$

Moreover, the 4-way handshake in our scheme is modified as Fig. 4.

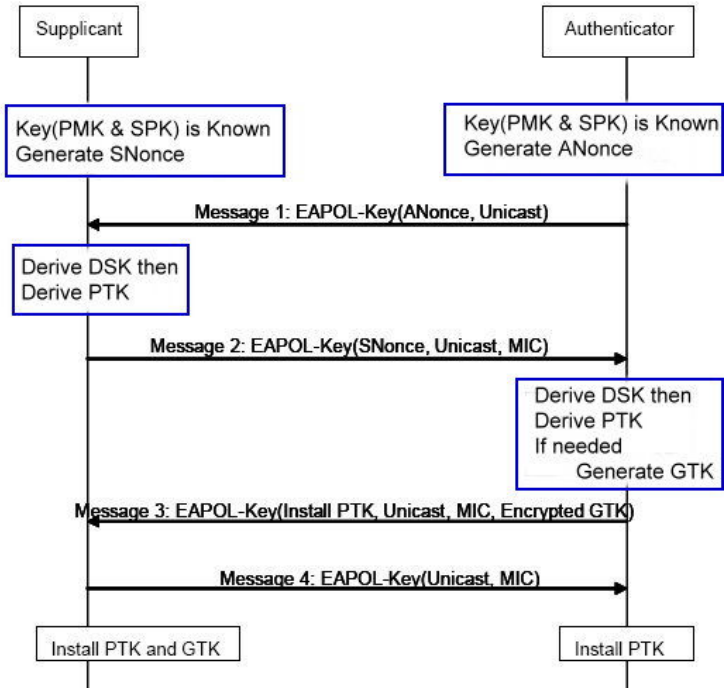


**Fig. 4.** 4-way handshake in MKE scheme

### 3.2 The whole encryption process with MKE

In IEEE 802.11i, the standard provides many solutions to secure the wireless communications. Consider a long tern solution, we discuses using 802.1X to do the authentication. Then in key management state, we use our MKE scheme to enhance it. Finally, the data is encrypted by Counter-mode/CBC-MAC Protocol (CCMP).

Hence, in our scheme, the authentication follows the standard and we using EAP-TLS with radius server (AS) to implement it. The complete process is illustrated as Fig. 5 and Fig. 6.

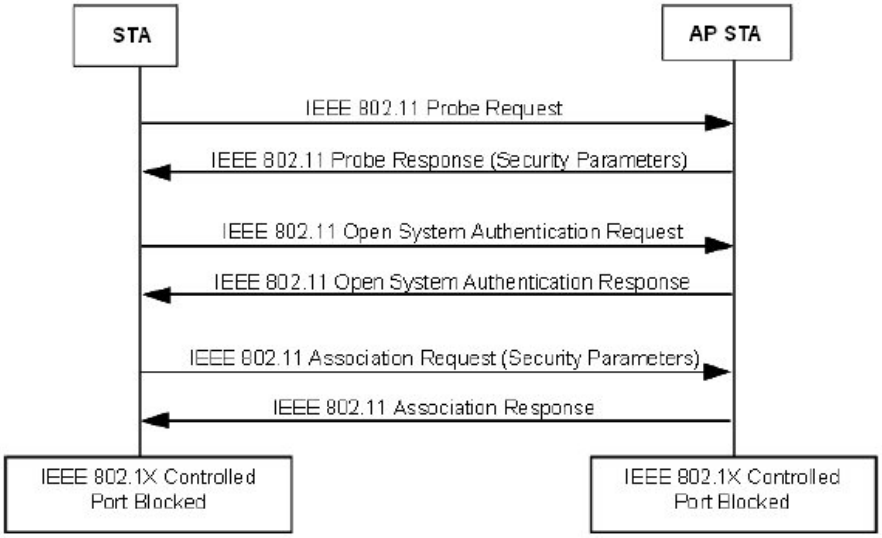


**Fig. 5.** Establishing the IEEE 802.11 association

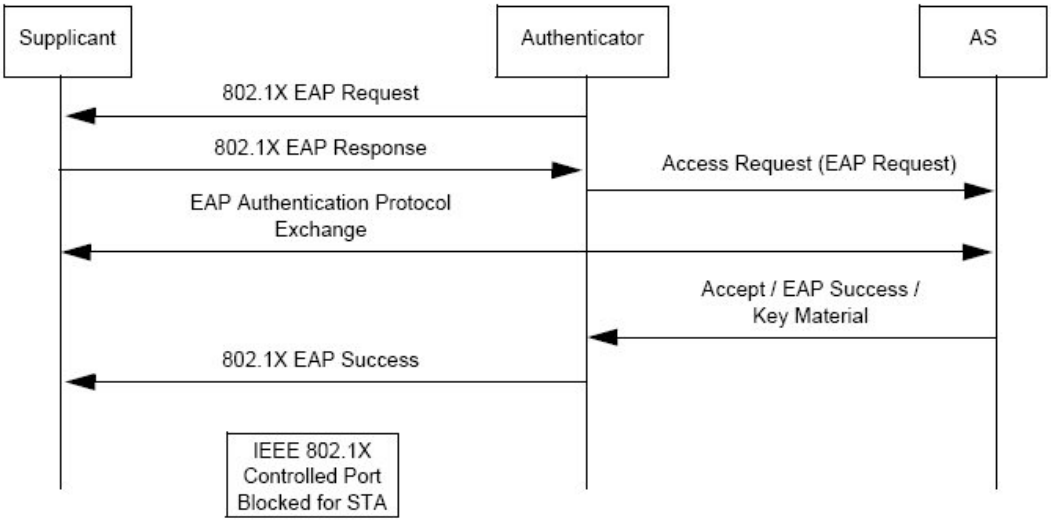


**Fig. 6.** IEEE 802.1X EAP authentication

After successful EAP authentication, both supplicant and authenticator hold the same PMK. Moreover, these two ends have the same SPK which we install in the initial state as well. Then it will perform the MKE 4-way handshake as Figure 2 to periodically refresh PTK. We do not change the architecture of PTK. Hence, the hierarchy of PTK (pairwise transient key) is as Figure 7.

| Pairwise Transient Key (PTK) (384bits) | | |
|---|---|---|
| Key Confirmation Key (KCK)<br>0 bit~127 bit (128bits) | Key Encryption Key (KEK)<br>128bit~255bit (128bits) | Temporal Key (TK)<br>256bit~383bit (128bits) |

**Fig. 7.** PTK architecture

Finally, in data encryption state, we follow the IEEE 802.11i standard which is using AES-CCM algorithm to provide data confidentiality, integrity and replay protection. The procedure of AES-CCM encryption is shown as Fig. 8.

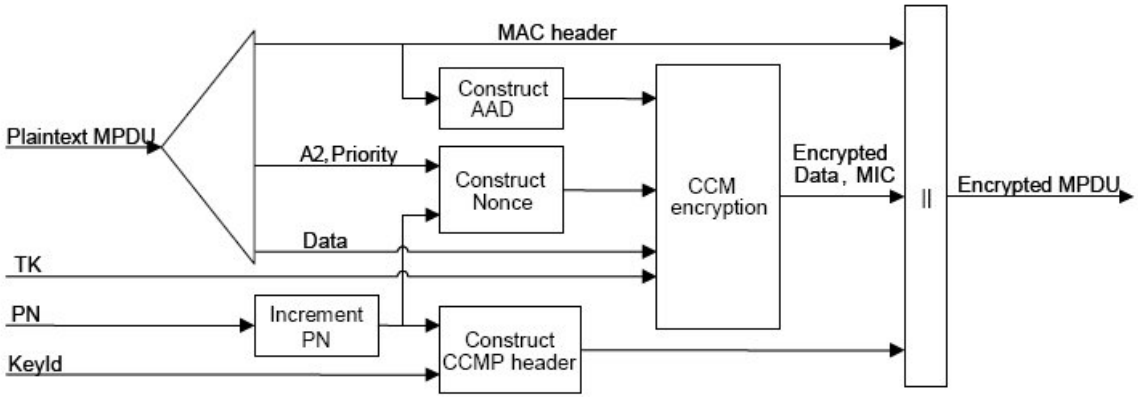


**Fig. 8.** AES-CCM encryption procedure

### 3.3 The effectiveness and secrecy of MKE

MKE just modify the key management state without changing data encryption algorithm. Therefore, the encrypted data payload is the same as WPA2. The only additional overhead is that we use two hash functions to compute the PTK during 4-way handshake. However, this handshake procedure just executes periodically. Hence, the computation overhead of the system is small enough to neglect, we enhance WPA2 security mechanism without producing too much overhead.

## 4 Correctness Proof of Algorithm

In order to proof the correctness of our scheme, we employ the protocol composition logic (PCL) [38] which contains three main component as modeling protocols, protocol logic with the proof system and compositional proof method. This system is proposed by security laboratory in Stanford University [39, 40, 41]. Therefore, we won't describe the details about PCL here. Instead, we'll promote the extra axioms to suit our scenario. Finally, we'll apply this system to proof the Multi-Key Encryption (MKE) step by step.

### 4.1 A brief of the proof system and some axioms

This system contains some terms (variables), actions and axioms. The goal is to use these axioms and some assumption to derive the theories step by step. Finally, apply these theories to conclude the correctness of the protocol.

**Terms:**

| | |
|---|---|
| $c$ | constant term |
| $x$ | variable |
| $N$ | participator |
| $K$ | key |
| $t, t$ | tuple of terns |
| $SIG_K(t)$ | term signed with key $\overline{K}$ (private-key) |
| $ENC_K(t)$ | term encrypted with key $K$ (public-key) |
| $pmk$ | pairwise master key |
| $spk$ | second pre-share key |
| $dsk$ | derived second pre-share key |
| $ptk$ | pairwise transient key |

**Actions:**

| | |
|---|---|
| Send(A,m) | participator A executed action send m |
| Receive(A,m) | participator A receiving data m into variable m |

| | |
|---|---|
| New(A,m) | participator A generate a new data m |
| Encrypt(A, $ENC_K\{\|m\|\}$) | participator A encrypt data m with public-key $K$ |
| Decrypt(A, $ENC_K\{\|m\|\}$) | participator A decrypt data m with private-key $K$ |
| Sign(A, $SIG_K\{\|m\|\}$) | participator A using private-key $K$ to make a digital signature to data m |
| Verify(A, $SIG_K\{\|m\|\}$) | participator A executed the signature verification action verify $SIG_K\{\|m\|\}$ |

**Axioms:**

**AA1** $\varnothing[a]_X \Diamond$a

If a principal has executed an action in some role, then the corresponding predicate asserting that the action had occurred in the past is true.

**AA2** $Fresh(X,t)[a]_X \Diamond (a \wedge \Theta Fresh(X,t))$

no action predicate can hold if thread $X$ executed no actions

**AA4** $\varnothing[a;...;b]_X \Diamond a < b$

after thread $X$ does actions $a, \cdots, b$ in sequence, the action predicates, $a$ and $b$, corresponding to the actions, are temporally ordered in the same sequence.

**AN2** $\varnothing[(vn)]_X Has(Y,n) \supset (Y = X)$

**AN3** $\varnothing[(vn)]_X Fresh(X,n)$

If principal $X$ generates a new value n and does no further actions in this role, then axiom AN2 says that $X$ knows n and AN3 says that n is fresh.

**FS1** $Fresh(X,t)[Send\ t']_X\ FirstSend(X,t,t')\ where\ t \subseteq t'$

The predication $FirstSend(X,t,t')$ will hold if a thread $X$ sends the term $t'$ containing $t$ starting from a state where $t$ is fresh.

**FS2** $FirstSend(X,t,t') \wedge a(Y,t'') \supset Send(X,t') < a(Y,t'')\ where\ X \neq Y\ and\ t \subseteq t''$

If a thread $Y$ does some action with a term $t''$ which contains term $t$. The thread $X$ will send term $t$ which is inside term $t''$ before $Y's$ action.

**HASH1** $Computes(X, HASH_K(x)) \supset Has(X,x) \wedge Has(X,K)$

If $X$ can use a hash function with parameter $K$ and $x$ to compute a data, this implies $X$ has $x$ and $K$.

**HASH2** $Computes(X, HASH_K(x)) \supset Has(X, HASH_K(x))$

If $X$ can use a hash function with parameter $K$ and $x$ to compute a data, this implies $X$ has that hashed data.

**HASH3**
$$\text{Re}ceive(X, HASH_K(x)) \supset$$
$$\exists Y.Computes(Y, HASH_K(x)) \wedge Send(Y, HASH_K(x))$$

If $X$ receives a data $HASH_K(x)$, this implies there exist a participator $Y$ who can compute and send that data.

**HASH4**
$$Has(X, HASH_K(x)) \supset Computes(X, HASH_K(x)) \vee$$
$$\exists Y, m.\ Computes(Y, HASH_K(x)) \wedge Send(Y,m) \wedge Contains(m, HASH_K(x))$$

If $X$ has the data $HASH_K(x)$, it implies either $X$ can compute it by itself or there exist a participator $Y$ who can compute and send that data.

***Define*** $Computes(X, HASH_K(a)) \equiv Has(X,K) \wedge Has(X,a)$

According to HASH1 to HASH4, we can conclude that if $X$ can compute the data $HASH_K(a)$, this statement equals that $X$ has $K$ and $X$ has $a$.

**SPMK2 (for MKE 4-way)** $Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset (Has(\widehat{Z}, pmk) \wedge Has(\widehat{Z}, spk)) \supset \widehat{Z} = \widehat{X} \vee \widehat{Y}$

If $X$ and $Y$ are honest, then it implies that if there is a participator $Z$ has $pmk$ and has $spk$ then this participator is either $X$ or $Y$. (This axioms is especially for MKE 4-way handshake)

For more details please see [42]

### 4.2 Proof of the 4-way handshake guarantee in Multi-Key Encryption (MKE) scheme

Suppose $X$ is authenticator and $Y$ is supplicants.

The invariants of the system are as follows

$\theta_{4\omega\alpha y}$ $Has(\widetilde{X}, pmk, spk) \wedge Has(\widehat{Y}, pmk, spk) \wedge NonceSource(Y, pmk, ENC_{\bar{x}}(pmk))$

In 4-way handshake protocol, $X$ has $pmk$, $spk$ and $Y$ has $pmk$, $spk$ and $Y$ will use key $K$ to encrypt $pmk$.

$\Gamma_{4\omega\alpha y,1}$ $Computes(\widehat{X}, HASH_{pmk}(x, y)) \supset -(Send(\widehat{X}, m) \wedge Contains(m, HASH_{pmk}(x, y))$

If $X$ can use a hash function with parameter $pmk$, $x$ and $y$ to computes the data, it implies $X$ won't send out any message contains this data.

$\Gamma_{4\omega\alpha y,2}$ $(Honest(\widehat{X}) \wedge \text{Re}ceieve(X, Message1) \supset -(Send(X, Message3)) \wedge$
$(Honest(\widehat{X}) \wedge Send(X, Message1) \supset -(Send(X, Message2) \wedge Send(X, Message4)))$

If $X$ is honest and receives message1, that implies $X$ won't send out message3 and if $X$ is honest and send message1, that implies $X$ won't send message2 and message4.

**Then the detail of proof is as follows:**

**AA1 › ARP › AA4** $\theta_{4\omega\alpha y}$

$[4WAY : AUTH]_X$
$Send(X, \widehat{X}, \widehat{Y}, x, "msg1") <$
$\text{Re}ceive(X, \widehat{Y}, \widehat{X}, "msg2", HASH_{ptk}(y, "msg2")) <$
$Send(X, \widehat{X}, \widehat{Y}, x, "msg3", HASH_{ptk}(x, "msg3")) <$
$\text{Re}ceive(X, \widehat{Y}, \widehat{X}, "msg4", HASH_{ptk}("msg4"))$

**(1)**

**ARP › HASH3** $\theta_{4\omega\alpha y}$

$[receive\ \widehat{Y}, \widehat{X}, z;$
$match\ z/"msg4", mic2;\ match\ mic2 / HASH_{ptk}("msg4")]_X$
$\text{Re}ceive(X, \widehat{Y}, \widehat{X}, "msg4", HASH_{ptk}("msg4")) \supset$
$\exists Z.Computes(Z, HASH_{ptk}("msg4")) \wedge Send(Z, HASH_{ptk}("msg4")) \wedge$
$(Send(Z, HASH_{ptk}("msg4")) <$
$\text{Re}ceive(X, \widehat{Y}, \widehat{X}, "msg4", HASH_{ptk}("msg4"))$

**(2)**

**HASH1** $Computes(Z, HASH_{ptk}("msg4")) \equiv Has(\widehat{Z}, ptk) \wedge Has(\widehat{Z}, "msg4")$ **(3)**

**HASH4**

$$Has(\widehat{Z}, ptk) \equiv Has(\widehat{Z}, HASH_{pmk,dsk}(x,y)) \supset Computes(\widehat{Z}, HASH_{pmk,dsk}(x,y)) \vee (\exists Y, m.Computes(Y, HASH_{pmk,dsk}(x,y)) \wedge Send(Y,m) \wedge Contains(m, HASH_{pmk,dsk}(x,y)))$$

**(4)**

**(4)** , $\Gamma_{4\omega\alpha y,2}$

$$\theta_{4\omega\alpha y}$$

$$[Receieve\ \widehat{Y}, \widehat{X}, z; match\ z/"msg4", mic2;\ mic2/HASH_{ptk}("msg4")]_X$$

$$Has(\widehat{Z}, ptk) \equiv Has(\widehat{Z}, HASH_{pmk,dsk}(x,y) \supset Computes(Z, HASH_{pmk,dsk}(x,y))$$

**(5)**

**(5)** , **HASH1**

$$\theta_{4\omega\alpha y}$$

$$[Receieve\ \widehat{Y}, \widehat{X}, z; match\ z/"msg4", mic2;\ mic2/HASH_{ptk}("msg4")]_X$$

$$Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset Computes(Z, HASH_{ptk}("msg4")) \supset Has(\widehat{Z}, ptk) \supset Has(\widehat{Z}, pmk) \wedge Has(\widehat{Z}, dsk)$$

**(6)**

**(6)** , **HASH1**

$$Has(\widehat{Z}, dsk) \equiv Has(Z, HASH_{spk}(x,y)) \supset Computes(Z, HASH_{spk}(x,y))$$

**(7)**

**HASH1**

$$Computes(Z, HASH_{spk}(x,y)) \equiv Has(\widehat{Z}, spk)$$ **(8)**

**(6)** , **(8)** , **SMPK2**

$$Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset Has(\widehat{Z}, pmk) \wedge Has(\widehat{Z}, spk) \supset (\widehat{Z} = \widehat{X} \vee \widehat{Z} = \widehat{Y})$$

**(9)**

**AA1** , $\Gamma_{4\omega\alpha y,2}$

$$\theta_{4\omega\alpha y}$$

$$[new\ x; send\ \widehat{X}, \widehat{Y}, x, "msg1";]_X$$

$$Honest(\widehat{X}) \wedge Send(X, \widehat{X}, \widehat{Y}, x, "msg1") \supset \widehat{Z} \neq \widehat{X}$$

**(10)**

**(2)** , **(9)** , **(10)**

$$\theta_{4\omega\alpha y}$$

$$[4WAY : AUTH]_X$$

$$Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset \exists Z.Computes(Z, HASH_{ptk}("msg4")) \wedge Send(Z, HASH_{ptk}("msg4")) \wedge \widehat{Z} = \widehat{Y}$$

**(11)**

**(2)** , **(11)**

$$\theta_{4\omega\alpha y}$$

$$[4WAY : AUTH]_X$$

$$Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset Send(Y, \widehat{Y}, \widehat{X}, "msg4", HASH_{ptk}("msg4")) < \text{Re}ceive(X, \widehat{Y}, \widehat{X}, "msg4", HASH_{ptk}("msg4"))$$

**(12)**

**(12)**，$\varnothing HONESTY$ $\theta_{4\omega\alpha y}$

$$[4WAY:AUTH]_X$$
$$Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset$$
$$\mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg1") <$$
$$Send(Y,\widehat{Y},\widehat{X},y,"msg2",HASH_{ptk}(y,"msg2")) <$$
$$\mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg3",HASH_{ptk}(x,"msg3")) <$$
$$Send(Y,\widehat{Y},\widehat{X},"msg4",HASH_{ptk}("msg4"))$$

**(13)**

**(13)**，**HASH3** $\theta_{4\omega\alpha y}$

$$[4WAY:AUTH]_X$$
$$\mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg3",HASH_{ptk}(x,"msg3")) \supset$$
$$\exists Z.Computes(Z,HASH_{ptk}(x,"msg3")) \wedge$$
$$Send(Z,HASH_{ptk}(x,"msg3")) \wedge$$
$$(Send(Z,HASH_{ptk}(x,"msg3")) <$$
$$\mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg3",HASH_{ptk}(x,"msg3")))$$

**(14)**

**HASH1**，**(5)**，**(9)** $\theta_{4\omega\alpha y}$

$$[4WAY:AUTH]_X$$
$$Computes(Z,HASH_{ptk}(x,"msg3")) \supset Has(\widehat{Z},ptk) \supset$$
$$\widehat{Z}=\widehat{X} \vee \widehat{Z}=\widehat{Y}$$

**(15)**

$\Gamma_{4\omega\alpha y,2}$ $\theta_{4\omega\alpha y}$

$$[4WAY:AUTH]_X$$
$$Honest(\widehat{Y}) \wedge \mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg1") \supset \widehat{Z} \neq \widehat{Y}$$

**(16)**

**(14)**，**(15)**，**(16)** $\theta_{4\omega\alpha y}$

$$[4WAY:AUTH]_X$$
$$\widetilde{Honest}(X) \wedge \widetilde{Honest}(Y) \supset$$
$$\exists Z.Computes(Z,HASH_{ptk}(x,"msg3")) \wedge$$
$$\widetilde{Send}(Z,HASH_{ptk}(x,"msg3")) \wedge \widetilde{Z=X}$$

**(17)**

**(14) ‣ (17)**

$$\theta_{4\omega\alpha y}$$

$$[4WAY:AUTH]_X$$

$$Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset$$

$$Send(X,\widehat{X},\widehat{Y},x,"msg3",HASH_{ptk}(x,"msg3")) <$$

$$\mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg3"),HASH_{ptk}(x,"msg3"))$$

**(18)**

**FS1 ‣ AN3**

$$\theta_{4\omega\alpha y}$$

$$[4WAY:AUTH]_X$$

$$Honest(\widehat{Y}) \supset FirstSend(Y,y,\widehat{Y},\widehat{X},y,"msg2",HASH_{ptk}(y,"msg2"))$$

**(19)**

**(19) ‣ FS2**

$$\theta_{4\omega\alpha y}$$

$$[4WAY:AUTH]_X$$

$$Send(Y,\widehat{Y},\widehat{X},y,"msg2",HASH_{ptk}(y,"msg2")) <$$

$$\mathrm{Re}ceive(X,\widehat{Y},\widehat{X},y,"msg2"),HASH_{ptk}(y,"msg2"))$$

**(20)**

**FS1 ‣ AN3**

$$\theta_{4\omega\alpha y}$$

$$[new\ x; send\ \widetilde{X},\widetilde{Y},x,"msg1";]_X$$

$$FirstSend(X,x,\widetilde{X},\widetilde{Y},x,"msg1")$$

**(21)**

**(21) ‣ FS2**

$$\theta_{4\omega\alpha y}$$

$$[4WAY:AUTH]_X$$

$$Send(X,\widehat{X},\widehat{Y},x,"msg1") < \mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg1")$$

**(22)**

**(1,12,13,18,20,22)**

$$\theta_{4\omega\alpha y}$$

$$[4WAY:AUTH]_X$$

$$Honest(\widehat{X}) \wedge Honest(\widehat{Y}) \supset$$

$$Send(X,\widehat{X},\widehat{Y},x,"msg1") < \mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg1") <$$

$$Send(Y,\widehat{Y},\widehat{X},y,"msg2",HASH_{ptk}(y,"msg2")) <$$

$$\mathrm{Re}ceive(X,\widehat{X},\widehat{Y},y,"msg2",HASH_{ptk}(y,"msg2")) <$$

$$Send(X,\widehat{X},\widehat{Y},x,"msg3",HASH_{ptk}(x,"msg3")) <$$

$$\mathrm{Re}ceive(Y,\widehat{X},\widehat{Y},x,"msg3",HASH_{ptk}(x,"msg3")) <$$

$$Send(Y,\widehat{Y},\widehat{X},"msg4",HASH_{ptk}("msg4")) <$$

$$\mathrm{Re}ceive(X,\widehat{Y},\widehat{X},"msg4",HASH_{ptk}("msg4"))$$

**(23)**

**QED.**

# 5 Implementation & Experiment

In this section, we implement MKE mechanism as we proposed above. We will use some methods which are usually adopted in wireless network to attack the standard and our secure mechanism individually. Finally, we compare results of two mechanisms.

## 5.1 Attack System Implementation

There are a lot of weaknesses and attack methods, such as FSM attack [23], PTW attack [43], Fragmentation attack [44], dictionary attack and so on. Some hackers implement those theories to applications, such as Aircrack, and so on. They share those applications free on the web, so everyone can get easily. We also use those applications to do experiment.

We implemented the attack system based on the Aircrack. The procedures of attacking system are as Fig. 9. First, our system will scan the APs and end users within coverage range. Then it will choose the target AP to crack and send de-authentication packet to its clients. Right after that, it can capture the 4-way handshake packet since the clients doing re-authentication. Finally, it can use these 4-way handshake messages with a dictionary file to compute and crack the key.

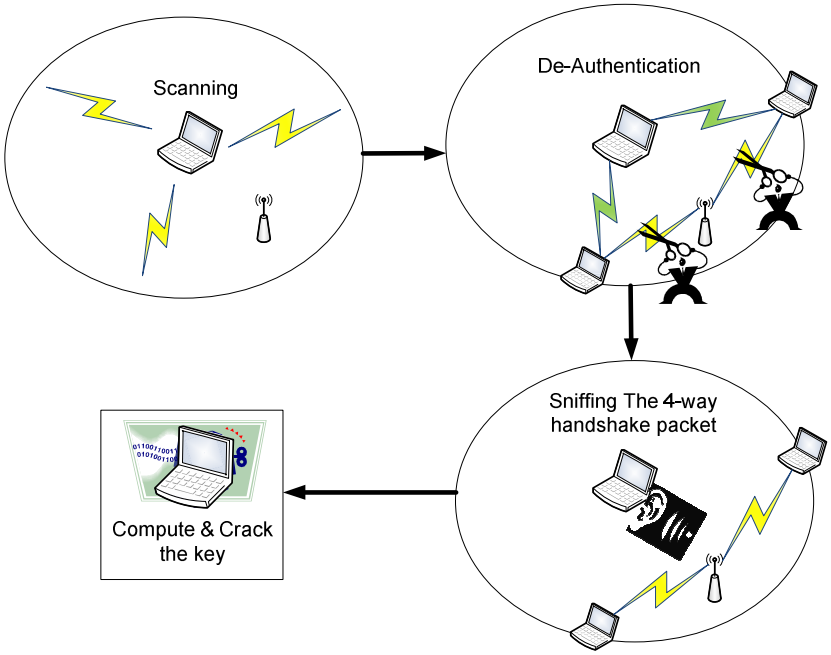


**Fig. 9.** Cracking Procedure of Attack System

## 5.2 MKE Implementation

To get and modify source codes easily, we use Linux-based OS to implement. We setup two PCs as AP and client (supplicant). We want one of PCs to play the role of AP, so we use the module called "hostapd" to do it. Then, we install "wpa_supplicant" to the other PC for supporting WPA. We implement MKE mechanism by modifying these two modules. The relative equipment information is as following tables (Table 1, Table 2):

**Table 1.** Client's equipment and related module

| Client's Equipment | |
|---|---|
| OS | Fedora Core 7 |
| Wireless NIC's chip | Atheros |
| WPA/WPA2 function | wpa_supplicant |

**Table 2.** AP's equipment and related module

| Access Point's Equipment | |
|---|---|
| **OS** | **Ubuntu 7.04** |
| **Wireless NIC's chip** | **Atheros** |
| **AP function** | **HostAP** |

The following is the pseudo code of our modification:

DSK: 32-byte Derived Second Pre-shared Key
SPK: 32-byte Second Pre-shared Key
PTK: 48-byte or 64-byte Pairwise Transient Key
PMK: 32-byte Pairwise Master Key

**Part of wpa_supplicant:**

```
program first_step_of_4_way_handshake ()
begin
...
generate Snonce
...
if adopt MKE mechanism
  DSK := sha1_prf(SPK,"Pairwise key expansion", Anonce);
  PTK := wpa_pmk_to_ptk(PMK, "Pairwise key expansion", Supplicant MAC
                        Address, AP MAC Address, Snonce, DSK);
else
  PTK := wpa_pmk_to_ptk(PMK, "Pairwise key expansion", Supplicant MAC
                        Address, AP MAC Address, Snonce, Anonce);
...
end
```

First step of 4-way handshake is that AP sends Anonce to the supplicant. Second, the supplicant generates a Snonce, and then it would adopt MKE mechanism to generate PTK or not. If we don't adopt MKE mechanism, the supplicant will compute PTK in standard mechanism by using PMK, a static string, supplicant's MAC address, AP's MAC address, Snonce, and Anonce. If we adopt MKE mechanism, the supplicant will use Anonce, SPK and a static string to compute DSK by sha1 hash function. Then, it adopts standard mechanism to compute PTK which DSK replaces the position of Anonce.

**Part of hostapd:**

```
program second_step_of_4_way_handshake ()
begin
...
if adopt MKE mechanism
  DSK := sha1_prf(SPK,"Pairwise key expansion", Anonce);
  PTK := wpa_pmk_to_ptk(PMK, "Pairwise key expansion", Supplicant MAC
                        Address, AP MAC Address, Snonce, DSK);
else
  PTK := wpa_pmk_to_ptk(PMK, "Pairwise key expansion", Supplicant MAC
                        Address, AP MAC Address, Snonce, Anonce);
...
end
```

Second step of 4-way handshake is that the supplicant sends Snonce to AP. At this time, the action is similar with the part of wpa_supplicant but AP doesn't need to generate Snonce.

### 5.3 Experimentation Environment and Results

Our experimentations include two parts as below:

Experimentation I:

1. Secure mechanism uses standard WPA-PSK.

2. AP and clients share the same key “12345678”.
3. The word “12345678” is in our dictionary.

We monitor the packets of the AP and wait for the 4-way handshake packets. When we capture the packet, we use the packet to do dictionary attack. Because the word “12345678” is included in the dictionary, so we can crack and retrieve the key successfully (Fig. 10).

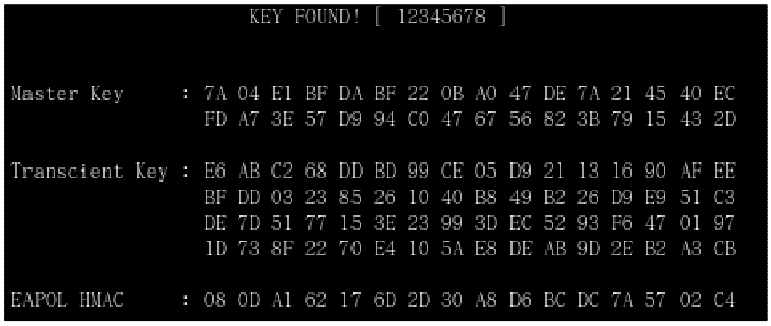


**Fig. 10.** Experimentation I result

Experimentation II:
1. Secure mechanism uses our MKE.
2. AP and clients share two key “12345678” and “12345678”.
3. The word “12345678” is in our dictionary.

We monitor the packets of the AP and wait for the 4-way handshake packet. When we capture the packet, we use the packet to do dictionary attack. Although “12345678” is in the dictionary, we can’t succeed to crack and get the key (Fig. 11).

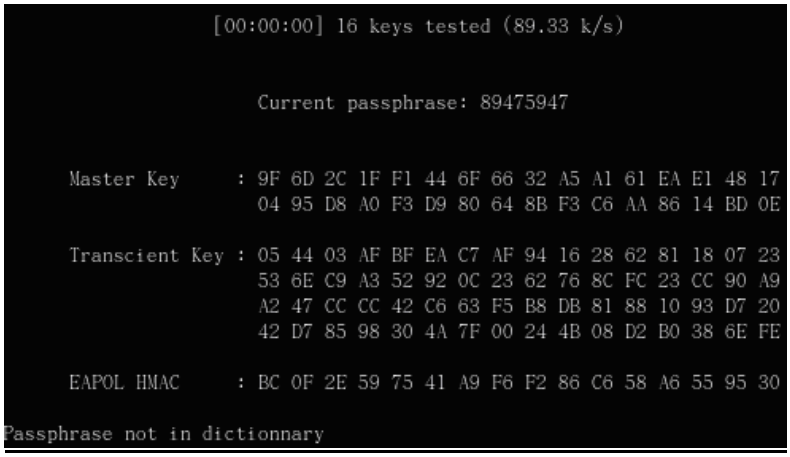


**Fig. 11.** Experimentation II result

## 6 Conclusion and Future Work

Next Generation Wireless Networks will be expected to support numerous mobile applications and provide ubiquitous computing environment. As more and more activities evolve in the wireless network, the security of confidential data and individual privacy will become a key issue. In order to provide and satisfy the requirements of mobility and security for NGWN, we propose a three years project, named Secure Mobile Service for Next Generation Wireless Network (SMS-NGWN).

In the current stage, we mainly propose Multi-Key Encryption mechanism to solve key management issues of current WLAN security mechanisms. MKE just modified the key management state and didn’t change data encryption algorithm. So the encrypted data payload is the same as WPA2. The only additional overhead is that we using two hash functions to compute the PTK during 4-way handshake. Thus, we enhance WPA2 security

mechanism without producing much overhead and validate its correctness through the formal proof and the experimentation.

Our future work will continue on the WiMAX network security and heterogeneous network security. We notice that WiMAX's authorization key also suffers from dictionary attack. Thus, in the second stage, we will adopt the MKE concept to enhance the key management part of WiMAX system. Finally, heterogeneous network security will be considered. Since NGWN is an integrated network architecture, a well designed security policies should be developed in traditional cellular system and dynamic ad hoc system as well.

## 7 Acknowledgement

This work was supported by Institute of Information Industry under the "Wireless Broadband Communication Technology & Application Plan" project and National Science Council under the "Robokid" project.

## References

[1] Keith Holt , "Wireless LAN: Past, Present, and Future," *IEEE Computer Society*, Vol. 3, March 2005, pp. 92-93.

[2] Sasha Dekleva, J.P. Shim, Upkar Varshney, Geoffrey Knoerzer, "Evolution and emerging issues in mobile wireless networks," *ACM Press*, Vol. 50, No. 6, June 2007, pp. 38-43.

[3] ITU-T Recommendation Y.2001, "General overview of NGN," Dec. 2004.

[4] Kaveh Pahlavan, Prashant Krishnamurthy, "Principles of Wireless Networks: A unified Approach," *Pearson Education*, *Prentice Hall PTR*, 2002.

[5] William Stalling, "Cryptography and Network Security:Principles and Practices, 3rd edition," *Pearson Education, Prentice Hall PTR*, 2003.

[6] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Mails, "A Framework for IP Based Virtual Private Networks", RFC-2764, February 2000.

[7] Adrian Leunga, Yingli Sheng, Haitham Cruickshank, "The security challenges for mobile ubiquitous services," *Elsevier Information Security Technical Report*, Vol. 12, No. 3, Jan. 2007, pp. 162-171.

[8] Biju Issac, Seibu Mary Jacob and Lawan A. Mohammed, "The Art of War Driving and Security Threats -A Malaysian Case Study," *IEEE International Conference on Networks*, Vol. 1, Nov. 2005.

[9] "Wi-Phishing" and "Evil Twins" at Hotspots How to secure your mobile workforce, *AirDefense White Paper*, 2005

[10] IEEE Standard 802.11-1999, IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *IEEE Press*, 1999.

[11] J. R. Walker, "Unsafe at any key size; An analysis of the WEP encapsulation", *Intel Corporation*, doc. IEEE 802.11-00/362, October 2000.

[12] A. Stubblefield, J. Ioannidis, A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", *AT&T Labs Technical Report TD–4ZCPZZ*, August 2001.

[13] S. Fluhrer, I. Mantin and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", in *8th Annual Workshop on Selected Areas in Cryptography*, Vol. 2259, August 2001, pp. 1-23.

[14] IEEE Std 802.11i/D4.1, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium

Access Control (MAC) Security Enhancements," July 2003

[15] A. Bakirdan, J. Qaddour and I.K. Jalozie, "Security algorithms in Wireless LANs: Proprietary or non Proprietary", *IEEE Globecom,* Vol. 3, 2003, pp. 1425-1429.

[16] IEEE 802.11i/D4.1 (D6), "Draft Supplement to IEEE Std 802.11. Part 11: Specifications for Enhanced Security", IEEE draft, July (September), 2003.

[17] J. Park, and D. Dicoi, "WLAN Security: Current and Future", *IEEE Internet Computing*, Vol.7, No. 5, September – October, 2003, pp. 60-65.

[18] IEEE Std 802.1x, Port-based Network Access Control, June 2001.

[19] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed, "Extensible Authentication Protocol (EAP)," RFC 3748, June, 2004

[20] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June, 2000.

[21] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol," IETF RFC 3588, September, 2003.

[22] J. Edney and W.A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i," *Addison-Wesley*, 2004.

[23] Robert Moskowitz, Weakness in Passphrase Choice in WPA Interface, November 4, 2003. http://www.wifinetnews.com/archives/002452.html

[24] John L. MacMichael, "Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode," *Linux Journal*, Vol. 2005, No. 137, September 2005.

[25] Takehiro Takahashi, WPA Cracker tool, available via website: http://www.tinypeap.org/wpa_cracker.html.

[26] Josh Wright, coWPAtty, available via website: http://www.wirelessdefence.org/Contents/coWPAttyMain.htm.

[27] John Bellardo, Stefan Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," *USENIX Security Symposium,* 2003, pp. 15-28.

[28] IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks, part 16: Air Interface for Fixed Broadband Wireless Access Systems, *IEEE Press*, 2001.

[29] IEEE 802.16-2004, IEEE Standard for Local and metropolitan area networks part 16: Air Interface for Fixed Broadband Wireless Access Systems, *IEEE Press*, 2004.

[30] IEEE Std 802.16e, IEEE Standard for Local and Metropolitan Area Networks, part 16, Air Interface for Fixed and Mobile Broadband Wireless Access Systems, *IEEE Press*, February 2006.

[31] Carl Eklund, Roger B. Marks, Kenneth L. Standwood and Stanley Wang, "IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access," *IEEE Communications Magazine*, Vol. 40, No. 6, June 2002, pp. 98-107.

[32] David Johnston, Jesse Walker, "Overview of IEEE 802.16 Security," *IEEE Security & Privacy*, May/June 2004.

[33] Fan Yang, Huaibei Zhou, Lan Zhang, Jin Feng, "An Improved Security Scheme in WMAN based on IEEE Standard 802.16", *0-7803-9335-X/05 2005 IEEE*

[34] Avi Freedman, Zion Hadad, Handoff Schemes Overview and Guidelines for handoff Procedures in 802.16, IEEE

C802.16sgm-02/24, 2002.

[35] Jeff Mandin, 802.16e Privacy Key Management (PKM) version 2, IEEE C802.16e-02/131r1, 2002

[36] Feng Tian, DongXin Lu, Rui Li, "Comment on Security Roaming of Key association for Fast Handover," C802.16e-04/571r1, 2005.

[37] Aircrack-ng tool, available via website: http://www.aircrack-ng.org/.

[38] Nancy Durgin, John Mitchell, and Dusko Pavlovic, "A compositional logic for protocol correctness," *IEEE Computer Security Foundations Workshop*, 2001, pp. 241-255.

[39] Stanford Security Lab website: http://crypto.stanford.edu/seclab/index.html

[40] A. Datta, A. Derek, J.C. Mitchell, D. Pavlovic, "A derivation system and compositional logic for security protocols," *Journal of Computer Security*, Vol.13, No.3, 2005, pp. 423-482.

[41] He, C., Sundararajan, M., Datta, A., Derek, A. and J. Mitchell, "A Modular Correctness Proof of IEEE 802.11i and TLS," *CCS '05*, November 7-11, 2005, pp. 2-15.

[42] Anupam Datta, Ante Derek, John C. Mitchell and Arnab Roy , "Protocol Composition Logic (PCL)," *Electronic Notes in Theoretical Computer Science,* Vol. 172, 2007, pp. 311-358.

[43] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin , "Breaking 104bit WEP in less than 60 seconds," *Cryptology ePrint Archive*, URL. http://eprint.iacr.org/2007/120.pdf , 2007

[44] Andrea Bittau , Mark Handley , Joshua Lackey, "The Final Nailin WEP's Coffin," *IEEE Security and Privacy*, 2006