ISSN 2319-2720

Volume 2, No.1, January – March 2013
International Journal of Computing, Communications and Networking
Available Online at http://warse.org/pdfs/2013/ijccn03212013.pdf

A Comparative study of Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) and Temporal Key Integrity Protocol (TKIP): *Wireless Security*

Margaret Kathing[1], Suchismita Bhattacharjee[2], Roshni Rajkumari[3]
[1]Assistant Professor, NERIST, Arunachal Pradesh,India, mgkathing@gmail.com
[2]Ph.D. Scholar, NERIST, Arunachal Pradesh, India, getsuchi87@gmail.com
[3]Ph.D. Scholar, NERIST, Arunachal Pradesh,India, rajkumari.roshni@gmail.com

ABSTRACT
With the increase in use of wireless network, the initial protocols, as first, Wireless Equivalent Privacy (WEP), then Wi-Fi Protected Access (WPA) was used to secure wireless communications. In this paper, a comparison study is carried out in between Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) and Temporal Key Integrity Protocol (TKIP). It is being studied that Advanced Encryption Standard (AES) is mandatory in both, but TKIP is a lower end encryption protocol and CCMP is a higher end encryption protocol.

Keywords: Wireless Network, AES, CCMP, TKIP, Mode of operation.

1. INTRODUCTION

In the realm of networking, there are various modes for attack on open wireless networks. It is substantially easier for some third person gain unauthorized access to the files and system on which we are using. In addition, it is possible that the attacker will analyze the traffic on your network, allowing him to see what sites you visit and to potentially steal your credentials for various sites. The attackers, instead of eves dropping on your network, but instead performs a denial of service attack. This type of attack floods the network with requests, making it incredibly difficult and in most cases impossible to access the internet and network.

With the development of technology, information is sent either through wired or wireless networks. This information needs to be protected for communication over these channels as the risk of losing this information is high. By applying encryption techniques, we can protect our information against attacks. Presently, continuous researches on new cryptographic algorithms are going on. However, it is very difficult to find out the specific algorithm, because we have already known that they must consider many factors like security, complexity,etc.

In this paper, CCMP is compared with TKIP on the basis of data frame, key length and block size. CCM mode is used to provide assurance of the confidentiality and authentication of computer data by combining the techniques of the counter (CTR) mode and the Cipher Block Chaining Message Authentication Code (CBC-MAC) algorithm.

The task group actually designed two protocols, one that would allow old WEP hardware to be upgraded, and another one that was made from scratch using the modern AES block cipher. These protocols were named TKIP and CCMP respectively.

WEP was developed in order to secure wireless network and provides security equivalent to the one that could be expected from a wired network. When WEP fails, TKIP was build around WEP to fix its flaws and to develop a reliable and compatible network security with the older equipments[2]. But after an extent, TKIP was discovered as having lots of weaknesses and the excitement in the field of study of wireless security started. Many new application areas came in focus which was more prone to the attacks on TKIP. Then an alternative wireless protocol came into focus as CCMP which was more reliable in terms of theory, abstraction, designs.

2. CCMP MODEL

2.1 Concept

The CCMP protocol is based on Advanced Encryption Standard (AES)[1]. Encryption algorithm is used by the Counter Mode with CBC–MAC (CCM) mode of operation. The CCM mode combines Counter (CTR) mode privacy and Cipher Block Chaining Message Authentication Code (CBC-

MAC) authentication. They provide good security and performance.[5]

CCMP was the second security protocol introduced as a replacement for WEP in the 802.11i amendment. CCM is a generic authenticate and encrypt block cipher mode. The full name of CCMP is Counter Mode with Cipher block Chaining Message Authentication Code Protocol. CCMP uses the AES block cipher for confidentiality, authentication and integrity and operates on the MPDU Level or on the Advanced Encryption standard (AES) algorithm currently specified in Federal Information Processing Standard (FIPS) Pub. 197[3], thus, CCM cannot be used with the Triple Data Encryption Algorithm [4], whose block size is 64 bits. CCM can be considered a mode of operation of the block cipher algorithm[4]. The security properties of CCM depend, at a minimum, on the secrecy of the key.

The input to CCM includes three elements:[3]

I. Data that will be both authenticated and encrypted called as the payload,
II. Associated data (that will be authenticated but not encrypted),
III. And a unique value, called a nonce, that is assigned to the payload and the associated data

CCMP produces a message integrity code (MIC) that provides data origin authentication and data integrity for the packet payload data. A packet number (PN) field, which is included in the CCMP header and incorporated into the encryption with MIC calculation, which provides replay protection.

CCM consists of two related processes: generation – encryption and decryption – verification, which combine two cryptographic primitives: counter mode encryption and cipher block chaining based authentication. Only the forward cipher function of the block cipher algorithm is used within these primitives.

In generation-encryption, cipher block chaining is applied to the payload, the associated data, and the nonce to generate a message authentication code (MAC), counter mode encryption is applied to the MAC and the payload to transform them into an unreadable form, called the ciphertext. Thus, CCM generation-encryption expands the size of the payload by the size of the MAC. In decryption-verification, counter mode decryption is applied to the purported ciphertext to recover the MAC and the corresponding payload; then, cipher block chaining is applied to the payload, the received associated data, and the received nonce to verify the correctness of the MAC. Successful verification provides assurance that the payload and the associated data originated from a source with access to the key.

The AES-CCMP cipher suite uses a 128-bit key for encryption and decryption. An AES-CCMP key can be one of the following:[8]

A. Pairwise key

This key is used for all packets sent by the 802.11 station, including unicast, multicast, and broadcast packets. This key is also used for all unicast packets received by the station.

The 802.11 station must support at least one pairwise key. For the pairwise key, the station must use either a key at index 0 in the default key table or a key-mapping key indexed by the media access control (MAC) address of the access point (AP) or peer station.

B. Group key

This key is used for all multicast and broadcast packets received by the 802.11 station.

Due to group key rotation, the 802.11 station must support at least two group keys. For the group keys, the station must use keys at index 1 through 3 in the default key table.

AES-CCMP keys are derived through a mutual pairwise master key (PMK) that can be statically defined (reshaped) on the 802.11 station or dynamically defined through a port-based authentication algorithm, such as IEEE 802.1X. The PMK is verified between the 802.11 station and the access point (AP) or peer station during the association operation.[9]

3. TKIP MODEL

3.1 Concept

TKIP stands for Temporal Key Integrity Protocol. When WEP was proved completely broken[6], a new security scheme for wireless networks was desperately needed. The Temporal Key Integrity Protocol (TKIP) was designed on top of WEP to fix all its known weaknesses. TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. TKIP uses the original WEP programming but "wraps" additional code at the beginning and end to encapsulate and modify it. Like WEP,

TKIP uses the RC4 stream encryption algorithm as its basis. The new protocol, however, encrypts each data packet with a unique encryption key, and the keys are much stronger than those of its predecessor

The TKIP cipher uses the following keys:[6]

1) 128 bit key for encryption and decryption.
2) 64 bit key for forgery protection through Message Integrity Code (MIC).

The TKIP key can be one of the following:

A. Pairwise key

This key is used for all packets sent by the 802.11 station, including unicast, multicast, and broadcast packets. The pairwise key is also used for all unicast packets received by the station.

The 802.11 station must support at least one pairwise key. For the pairwise key, the station must use either a key at index 0 in the default key table or a key-mapping key indexed by the media access control (MAC) address of the access point (AP).

B. Group key

This key is used for all multicast and broadcast packets received by the 802.11 station.

TKIP keys are derived through a mutual pairwise master key (PMK) that can be statically defined (preshared) on the 802.11 station or dynamically defined through a port-based authentication algorithm, such as IEEE 802.1X. The PMK is verified between the 802.11 station and the access point (AP) during the association operation.

Even though TKIP provides vastly improved security over the old WEP standard, it is still built using some of the same building blocks as WEP. TKIP has some weaknesses, most significantly the Message Integrity Code (MIC). Because of this, all new hardware supports the new and improved CCMP security standard.

The 802.11 2007 standard [5] defines four modifications of WEP that is made by TKIP.These are

1) The use of a new Message Integrity Check (MIC), which is generated by the keyed cryptographic algorithm Michael.
2) The MIC is, because of the design constraints, not very secure. Therefore TKIP implements countermeasures to handle this.
3) Replay protection, with the use of a per-MPDU TKIP sequence counter (TSC).
4) TKIP uses a cryptographic per-packet key mixing function to defeat weak-key attacks against the WEP key.

4. COMPARISION

A new security scheme called as TKIP was designed when WEP was degrading to fix all weakness for WEP. The TKIP has been developed in order to replace WEP, which still works on the WEP compatible hardware. It provides key mixing as an improvement over WEP. TKIP prevents replay attacks by using a sequence counter and rejecting out of order packet. The TKIP uses RC4 as its cipher because it needs to make sure that it would run on the WEP hardware.[6][7]

CCMP is an encryption protocol used in WPA2. Both TKIP and AES-CCMP has the same process of key management and creation. Figure1. shows the comparison of keys generation of TKIP and CCMP.

TKIP	CCMP
Temporal Keys	
Data encryption Key(128 bits)	Data encryption/Integrity key (128 bits)
Data integrity key(128 bits)	
EAPOL Key Encryption Key(128 bits)	EAPOL Key Encryption Key(128 bits)
EAPOL Key Integrity Key(128 bits)	EAPOL Key Integrity Key(128 bits)
Group keys	
Group Encryption Key(128 bits)	Group Encryption/Integrity key(128 bits)
Group Integrity Key(128 bits)	
Total key sizes	
768 bits	512 bits

Figure 1: Comparison between TKIP and CCMP

Although TKIP prevents many attacks that WEP was vulnerable for ,it is still vulnerable for other minor attacks like Beck-Tews and Ohigashi Morii attacks. CCMP is a totally different designed from WEP and TKIP. Beck-Tews attack is not again applicable to CCMP. But the CCMP does not apply attacks on EAPOL handshake.

The CCMP uses the AES which is now a government standard. Most RNSs use the AES-CCMP method of encryption due to cipher strength. Thus TKIP is considered secure but not as secure as CCMP.

5. CONCLUSION AND FUTURE SCOPE

TKIP is not directly comparable to AES, TKIP is an integrity check, AES is an encryption algorithm. In the context of wireless security this actually means TKIP vs 'AES based CCMP', where TKIP is a lower end encryption protocol and CCMP is a higher end encryption protocol. Thus, TKIP is considered secure but not as secure as CCMP. In future scope, there can be many better approaches for TKIP to come over the disadvantages over CCMP. This comparatable study can be brought under experimental conclusion.

REFERENCES

1. **Counter CBC-MAC Protocol (CCMP) Encryption algorithm**, 2003 Vocal Technologies ltd.
2. F. Michael Halvorsen and O. Haugen, **Crypanalysis of IEEE 802.11i TKIP**, Norwegian University, June 2009.
3. FIPS Publication 46-3, **Data Encryption Standard (DES)**, U.S. DoC/NIST, October 25, 1999.
4. G. Padmavathi et. al., **CCMP-AES Model with DSR routing protocol to secure Link layer and Network layer in Mobile adhoc Networks**, International Journal on Computer Science and Engineering, vol.2 No.5 2010.
5. **IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**, IEEE Standards 802.11-2007 (Revision of IEEE Standards 802.11-1999), 12 2007.
6. Scott Fluhrer, Itsik Mantin, and Adi Shamir, **Weaknesses in the key scheduling algorithm. In RC4**, Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography, pages 1–24, 2001.
7. S. Glass and V. Muthukkumarasamy, **A Study of the TKIP Cryptographic DoS Attack**, pages 59–65, Nov. 2007.
8. William Stallings, **Cryptography and Network Security: Principles and Practices**, Prentice Hall, 4th edition, 2006.
9. Edney and William A. Arbaugh, **Real 802.11 Security: Wi-Fi Protected Access and 802.11i**, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA- 2003.