Volume 2, No. 2, Mar-Apr 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

WLAN CCMP Protocol Nonce Enhancement using Transmission Rate

R.Buvaneswari*
Departments of IT &CT,
Hindustan College of Arts & Science,
Coimbatore 641 028,
buvana_ss@rediffmail.com

Dr.R.Balasubramanian
Dean, Academic Affairs
PPG Institute of Technology
Coimbatore 641 035
Catchrb@in.com

Abstract: IEEE has incorporated Counter Mode with Cipher Block Chaining Message Authentication Code protocol (CCMP) to provide robust security to IEEE 802.11 wireless LANs. Counter mode is used for data confidentiality and Cipher Block Chaining –Message Authentication Code (CBC-MAC) is used for data integrity and authentication. It is found that CCMP has been designed with a weak nonce construction and transmission mechanism, which leads to the exposure of initial counter value. This weak construction of nonce renders the protocol vulnerable to attacks by intruders. The failure of the counter mode will result in the collapse of the whole security mechanism of 802.11 WLAN.The IEEE 802.11 standard provides multiple data rates at the physical layer(PHY).The Physical Layer Convergence Protocol(PLCP) header specifies the data rate of current packet in SIGNAL field . This paper shows an enhancement to nonce through PLCP signal field. since signal rate is different for each transmission.

Keywords: CCMP, TKIP, WEP, nonce, IV, PLCP, transmission rate

I. INTRODUCTION

IEEE 802.11i incorporates authentication, data integrity and data encryption mechanisms to address security concerns for legacy and new wireless LANs in infrastructure and ad-hoc (peer-to-peer) based 802.11 networks. 802.11i specifies device authentication through IEEE 802.1X [2] and data security through the Wire Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP) or Counter Mode with CBC-MAC Protocol (CCMP). WEP and TKIP target legacy 802.11 equipment. Various academic and commercial studies have shown that WEP based WLAN Security can be breached by intruders. Vulnerabilities of WEP include weak encryption (short keys), static encryption keys and lack of key distribution mechanism. TKIP [1] provides counter-measures to possible attacks on WEP. The counter-measures reduce the probability of successful forgery and amount of information an attacker can learn about a key.

II. SECURITY FLAWS

Wireless networks are prone to different kind of security threats.[2] Ubiquitous RF signals provide conducive environment for malicious and well planned information warfare, where attackers can use the advance technology to mount attacks with the ease to sniff the MPDUs traversing the air. Generally the threats can be classified into the following:

**Leakage of Information:* Information dissemination to anyone who is not authorized to access it.

* *Alteration of Information:* Un-authorized or malicious alteration of data while in transit between autonomous systems, injection of spurious information using spoofing, replay of packets etc.

**Repudiation:* A party involved in the communication denies its involvement.

* *Impersonation:* An adversary pretends to be an authorized entity.

* *Service Stealing:* Unauthorized use of network or domain services without degrading the services to other users.

**Denial of Service:* Illegitimate access and intentional degradation or blocking of inter network communication links or services.

III. CCMP

By contrast, CCMP requires new 802.11 hardware with greater processing power. CCMP is based on the *Advanced Encryption Standard (AES)* [3], a FIPS-197 certified algorithm approved by NIST. AES (128 bits key length) operates in a counter mode (AES-128-CM) within 802.11i with CBC-MAC (CCM) [4] [5]. Counter mode is used for data confidentiality and Cipher Block Chaining – Message Authentication Code (CBC-MAC) is used for data integrity and authentication.[6] Counter mode operates by encrypting the initial counter and the resulting output is XORed with the plaintext to produce the cipher text . The initial counter is constructed from the flags field, length of the payload and the nonce.

A *Nonce*

The nonce is constructed from the packet number (PN), MAC layer A2 Address field (A2) and MAC layer priority field. Since the nonce value can be pre-computed, the only thing required to predict the counter value is length of payload. The length of the payload can be obtained through a priori information.

B. *CCMP Security Mechanism*

CCMP requires a fresh temporal key for every session. CCMP also requires a unique nonce value for each frame protected by a given temporal key, and CCMP uses a 48-bit packet number (PN) The CCMP headers concatenated with the MAC header, the encrypted payload, the encrypted MIC

© 2010, IJARCS All Rights Reserved

and the FCS field. These fields form the MPDU as illustrated in Figure 1 .

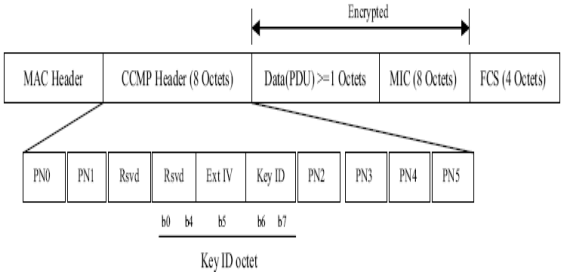

Figure 1 CCMP MPDU

The CCMP encapsulation process is depicted in Figure 2. CCMP encrypts[1] the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following steps :

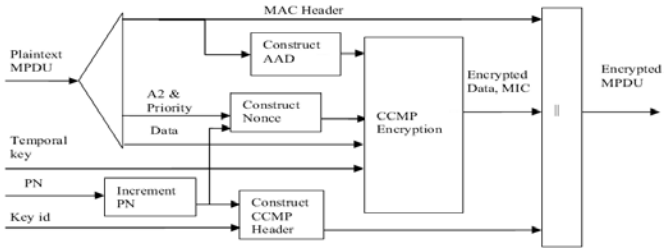

Figure 2 CCMP encapsulation block diagram

a) Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key. Note that retransmitted MPDUs are not modified on retransmission.

b) Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 when calculating the AAD.

c) Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2. The Priority field has a reserved value set to 0.

d) Place the new PN and the key identifier into the 8-octet CCMP header.

e) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing.

f) Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and MIC. [1]

The CCMP decapsulation steps are as follows:

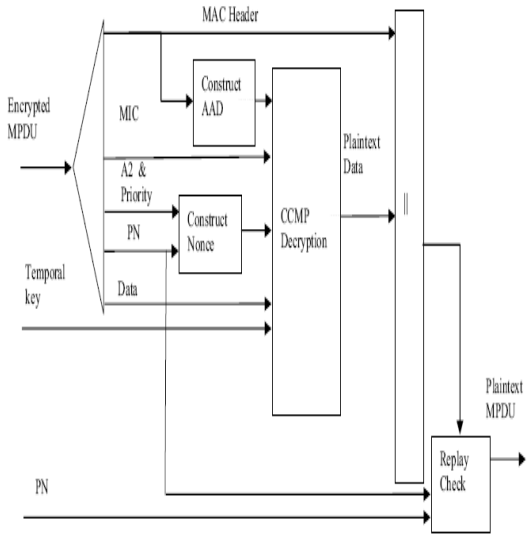

Figure 3 CCMP Decapulation block diagram

The decryption steps are:

a) The encrypted MPDU is parsed to construct the AAD and nonce values.

b) The AAD is formed from the MPDU header of the encrypted MPDU.

c) The nonce value is constructed from the A2, PN, and Priority Octet fields (reserved and set to 0).

d) The MIC is extracted for use in the CCM integrity checking.

e) The CCM recipient processing uses the temporal key, AAD, nonce, MIC, and MPDU cipher text data to recover the MPDU plaintext data as well as to check the integrity of the AAD and MPDU plaintext data.

f) The received MPDU header and the MPDU plaintext data from the CCM recipient processing may be concatenated to form a plaintext MPDU.

4. PHYSICAL LAYER CONVERGENCE PROTOCOL(PLCP)

A. *IEEE 802.11 Physical Layer(PHY)*

The IEEE 802.11 PHYs (physical layers) provide multiple transmission rates by employing different modulation and channel coding schemes.[9] For example, the 802.11b PHY provides 4 PHY rates from 1 to 11 Mbps at the 2.4 GHz band and most 802.11 devices available today in the market are based on this PHY.[10]. The PHYs have multiple data transfer rate capabilities that allow implementations to perform dynamic rate switching with the objective of improving performance. [7][1]

B. *Long PLCP PPDU Format*

The PLCP preamble contains the following fields: synchronization (Sync) and start frame delimiter (SFD). The PLCP header contains the following fields: signaling (SIGNAL), service (SERVICE), length (LENGTH), and CRC-16.

© 2010, IJARCS All Rights Reserved

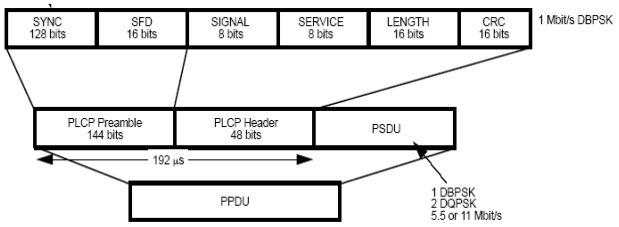

Figure 4 PLCP PPDU format

C. *PLCP SIGNAL field*

The 8-bit SIGNALfield indicates to the PHY the modulation that shall be used for transmission (and reception) of the PSDU. The data rate shall be equal to the SIGNAL field value multiplied by 100 kbit/s.[8] The High Rate PHY supports four mandatory rates given by the following 8-bit words, which represent the rate in units of 100 kbit/s, where the lsb shall be transmitted first in time:

a) X'0A' (msb to lsb) for 1 Mbit/s;
b) X'14' (msb to lsb) for 2 Mbit/s;
c) X'37' (msb to lsb) for 5.5 Mbit/s;
d) X'6E' (msb to lsb) for 11 Mbit/s.

D. *Reconstruction of Nonce in CCMP protocol*

The nonce block constitutes three fields. The first field is A2 address of MAC header (A2), second is priority field which is set to '0' by default and the third field is PN field.

Priority Field || Address (A2) || Packet Number (PN) = Nonce

The construction of nonce has been devised in such a manner that its reconstruction by an adversary is possible. The first 8 bits of nonce is the priority field which is presently kept as '0', this field may be used in future for 802.11 frame prioritization. The A2 field, which is 48 bits, is extracted from the MAC header field and is concatenated with the priority field. The only dynamic field, which is monotonically increasing per MPDU, is the PN field. The Reserved octet can be assigned with signal rate from PLCP or the 48 bit PN field can be reduced to 40bit PN field, an octet can be used to hold Signal field from PLCP header.

The enhancement to nonce block is as follows:

Priority Field || Address (A2) ||
Packet Number (PN) || signal rate from PLCP = Nonce

V. PROPOSED ARCHITECTURE

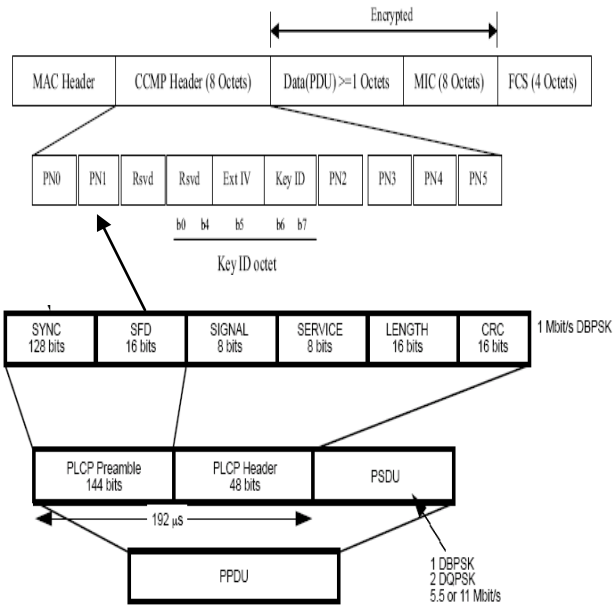

Figure 5. CCMP header nonce enhancement through PLCP protocol

The nonce is reconstructed from the packet number (PN), MAC layer A2 Address field (A2) , MAC layer priority field and signal field value from physical layer convergence protocol.

The Reserved octet can be assigned with signal rate from PLCP or the 48 bit PN field can be reduced to 40bit PN field, an octet can be used to hold Signal field from PLCP header. Dynamic nonce can be generated because signal rate value is different for each transmission based on the channel condition.

VI. **CONCLUSION:**

IEEE 802.11i has been well analyzed and recently CCMP protocol has been incorporated providing encryption, integrity and authentication. The counter mode has been used with AES to provide the confidentiality services. The mechanism, devised, is using the PN, A2, priority field and length of payload length to compute the counter value. This weak construction of nonce renders the protocol vulnerable to attacks by intruders.

The failure of the counter mode will result in the collapse of the whole security mechanism of 802.11 WLAN. The IEEE 802.11 standard provides multiple data rates at the physical layer(PHY).The Physical Layer Convergence Protocol(PLCP) header specifies the data rate of current transmission in SIGNAL field . Dynamic nonce can be generated because signal rate value is different for each transmission based on the channel condition.

VII. REFERENCES

[1] M.Junaid and Dr.Muidmutti," Vulnerabilities of IEEE 802.11i Wireless LAN CCMP protocol",World

© 2010, IJARCS All Rights Reserved

Academy of Science, Engineering and Technology,2005,P.No:408-412
[2] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.1X- 2001, "IEEE Standard for Local and metropolitan area networks – Port- Based Network Access Control" June, 2001.
[3] Specification for the Advanced Encryption Standard (AES), FIPS 197, U.S. National Institute of Standards and Technology. November 26,2001. [Online] Available: http://www.nist.gov/aes
[4] D. Whiting, R. Housley, and N. Ferguson. "Counter with CBC-MAC (CCM)". RFC 3610, September 2003.
[5] NIST Special Publication 800-38C, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality". May 2004. [Online] Available: http://csrc.nist.gov/publications/
[6] David A. McGrew, "Counter Mode Security: Analysis and Recommendations", Cisco Systems, November, 2002.
[7] IEEE Std. 802.11-1999, Part 11:Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specifications, Reference number ISO/IEC 8802-11:1999(E), IEEE Std. 802.11, 1999 edition, 1999.
[8] IEEE Std. 802.11b, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band, IEEE Std. 802.11b-1999, 1999.
[9] Jean-Lien C . Wu, Hunh-Huan Liu and Yi-Jen Lung, "An Adaptive Multirate IEEE 802.11 Wireless LAN," in Proc. 15th International Conference on Information Networking, 2001, pp. 411-418.
[10] Gavin Holland, Nitin Vaidya and Paramvir Bahl, "A Rate-Adaptive MAC Protocol for Multi-Hop Wireless Networks," in Proc. ACM SIGMOBILE'01, July 2001, pp. 236-
251.

AUTHORS:

Mrs.R.Buvaneswari received her B.Sc degree in Computer Science ,MCA at Bharathiar University, Coimbatore ,Tamil Nadu,INDIA. She completed M.Phil in computer Science at Mother Tesesa Women's University,Kodaikanal currenly pursuing her doctoral programme and She has 15 years Teaching and Research Experience and currently working as Head and Professor ,Department of Information Technology and Computer Technology,Hindusthan college of Arts and Science, Coimbatore,Tamil Nadu,India.

Dr. R. Balasubramanian was born in 1947 in India. He obtained his B.Sc., and M.Sc., degree in Mathematics from Government Arts College, Coimbatore, TamilNadu, in 1967 and PSG Arts College, Coimbatore, TamilNadu, in 1969 respectively. He received his Ph.D., from PSG College of Technology, Coimbatore, TamilNadu, in the year 1990. He has published more than 15 research papers in national and international journals. He has been serving engineering educational service for the past four decades. He was formerly in PSG College of Technology, Coimbatore as Assistant Professor in the Department of Mathematics and Computer Applications. He served as Associate Dean of the Department of Computer Applications of Sri Krishna College of Engineering and Technology, Coimbatore. Currently taken charge as Dean Academic Affairs at PPG Institute of Technology, Coimbatore, before which he was a Dean Basic Sciences at Velammal Engineering College, Chennai. He has supervised one PhD thesis in Mathematics and supervising four doctoral works in Computer Applications. His mission is to impart quality, concept oriented education and mould younger generation.

He is member of the board of studies of many autonomous institutions and universities. He was the principal investigator of UGC sponsored research project. He is a referee of an international journal on mathematical modeling. He has authored a series of books on Engineering Mathematics and Computer Science. He is a life member of many professional bodies like ISTE, ISTAM and CSI.

ll Rights Reserved