A MAC-LAYER SECURITY ARCHITECTURE FOR CABLE NETWORKS

Tadauchi Masaharu, Ishii Tatsuei, Itoh Susumu
Telecommunications Advancement Organization of Japan *Hitachi,Ltd,.* *Science University of Tokyo*

Abstract: Strengthened security is indispensable to the use of a cable network for e-commerce, the delivery of electronic public services, etc. This report proposes a new security system which better prevents tapping-related security violations. Enciphering in the system is on the Media Access Control (MAC) layer; including the MAC address among the enciphered items prevents the collection of information going to and coming from specific users by tapping. Simulation confirmed the operation of this system and its effectiveness.

Key words: cable network, MAC-layer, encryption protocol, symmetric cipher

1. INTRODUCTION

Cable networks are installed for the distribution of video information. In the tree topology of these networks the head-end of the cable access television (CATV) system is the root and the customers are the leaves. A unique Media Access Control (MAC) address is assigned to each device that is attached to the network and information is distributed by tagging it with these addresses. This allows each customer terminal to receive the appropriate information from the head-end.

Encryption is indispensable to the provision of e-commerce facilities, electronic public services, etc., over such a network. However, catching the MAC address of a device allows the monitoring of information thus tagged. It will be possible to crack any encryption of this information given enough time. This allows tapping. We propose a new system that makes it

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35612-9_23

B. Jerman-Blaži et al. (eds.), *Advanced Communications and Multimedia Security*

impossible for a tapper to distinguish data according to the customer. The MAC address is simply included among the items that are enciphered—we call this the CNMS (Cable Network MAC-layer Security) system. We have confirmed the operation of the system by simulation; the simulation also implied that CNMS provides superior security against tapping.

2. SYSTEM REQUIREMENTS

In considering a system to prevent the tapping of cable networks, we must start by considering the sources of this threat.

The tree topology of a cable network makes it possible to extract any information at any point in the network; it is easy to collect information going to and from the terminals of specific customers by using the MAC addresses and IP addresses that identify the terminals. These addresses should thus also be enciphered. The possibility of tapping remains, however, when a key is stolen, loaned, etc.

In table 1, required levels of security, i.e., of the use of cryptographic keys to prevent the cracking of tapped data, are classified into three levels according to the attack potential of aggressors which each must able to repel. A qualitative partition in terms of the attack potential is possible at level 2. This is discussed in section 5. There are fundamental differences between the offensive techniques employed by amateurs and professionals (pros): for example, an amateur is more likely to use monitored data to directly solve the encryption but a pro. tends to have a way of getting the key. A less talented amateur might also be able to receive a key. Obtaining a key is represented by level 1, the highest attack potential.

Table 1. Attack potential

Attack Level	Attackers	Notes	Definition
1	(Pro.) Group	Pro: is given the means for the attack. Am.: takes advantage of situations.	The acquisition of a key. Defense is difficult.
2	Solo Genius Group	Capital and situation are the limitations here; all available techniques are used. The aims are tapping and imposture.	Propriety of information collection for decryption →differences in the required level of defense.
3	Solo (Am.)	From the technically naïve to engineers; attackers who are not particularly interested in tapping or imposture.	It monitors by setup which PC mistook.

Pro.: Professional, one whose occupation involves tapping and imposture.
Teams of thieves, agents from government organizations, detectives, etc.
Am.: Amateur, one whose occupation is independent of tapping and imposture.

Level 1: The attackers are able to obtain encryption keys;
Level 2: The attackers have tools for solving encryption keys; and
Level 3: One who is not especially interested in tapping and carries out no special action.

3. SYSTEM DESIGN

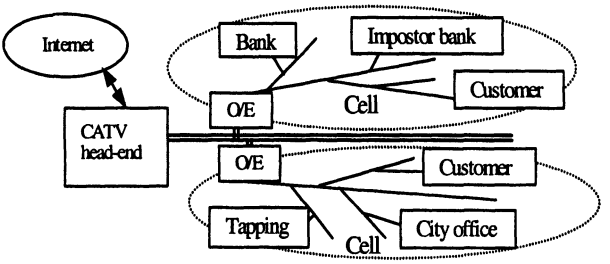

Figure 1. A cable network in the HFC configuration
(O/E: opto-electronic and electro-optic signal convertor)

The architecture of the CNMS system is described in this section. Fig. 1 shows an example of a cable network in the HFC (hybrid fiber/coax.) configuration. Several 'cells', each containing something in the region of 500 to 2,000 terminals, are connected with the CATV head-end by optical fiber. The tree topology within the cell is formed by coaxial cable.

A cell is set up for either symmetrical or non-symmetrical communication among its modems by the combination of the CMTS (cable modem termination system) at the CATV head-end and the CM (cable modem) operated by the customers. Upstream data and downstream data are always assigned to separate frequency bands. In a symmetrical modem system, upstream data are frequency-converted into downstream data before they are input into the CMTS at the CATV head-end. This allows peer-to-peer communications among terminals and sets of terminals within the cell. The target and originating terminals are represented in data flowing downstream and upstream, respectively, and this information is easy to intercept.

In the case of non-symmetry, communications are one-to-N from the CMTS to sets of N CMs and N-to-one from the sets of N CMs to the CMTS. An asymmetrical modem is described in DOCSIS 1.0 or 1.1 [1]. The downstream information on the network is still distributed to all of the terminals in a cell. Realizing encryption that encompasses the MAC address in a symmetrical modem-based system complicates the management of keys in the CM. Implementation is thus difficult. The CNMS proposed here is for systems based on asymmetrical modems.

3.1 Overview of the CNMS

The CNMS (Fig. 2) adds a security function to asymmetrical type modems such that encryption is realized in the MAC layer. In the PDU (Protocol Data Unit) format, the destination source MAC addresses are included among the items enciphered by the CNMS. This prevents the identification by tappers of specific subscribers as targets.

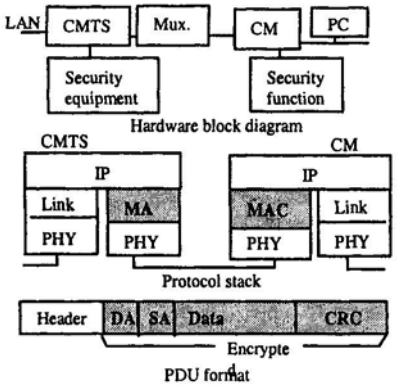

Figure 2. Concept of the CNMS

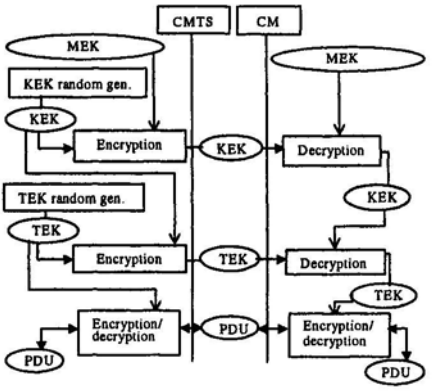

Figure 3. Arrangement of keys for the CNMS

Fig. 3 is a schematic diagram of the arrangement of keys at the CATV-head and customer ends when using symmetric cipher keys in carrying out an encrypted communication. The master encryption key MEK is placed as the symmetric cipher at both ends of the communication and is used to encipher and decipher the randomly generated key- and traffic-encryption keys, KEK and TEK. The TEK is used to encipher the transmission. All data within the cable network are enciphered in this way. Moreover, each key xEK has a lifetime L which follows L(MEK)>L(KEK)>L(TEK).

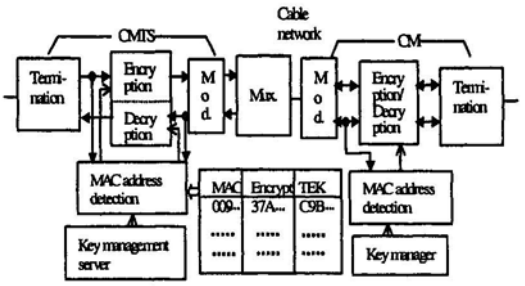

Figure 4. Block diagram of the CNMS

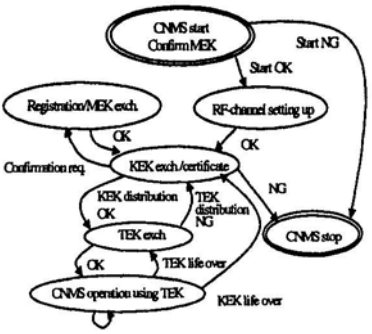

Figure 5. State transition diagram for the CNMS of a CM

3.2 Configuration and Operation of the CNMS

A block diagram of the proposed CNMS system is given as Fig. 4. A single key is in use in the cable modem (CM) of each customer; this allows satisfactory performance in decryption even with data sent at 30 Mbps. The CATV head-end, however, holds the keys for many customers, and having it individually and sequentially decrypt all of the data is not practicable. The MAC addresses as encrypted by the respective CM keys at a given time are thus memorized in a table which is part of the MAC address detection equipment of the CMTS at the CATV head-end. When a MAC address as encrypted by a CM is received at the head-end, the CMTS refers to this table to immediately identify the key. Fig. 4 shows the case where the encrypted MAC address is immediately detectable by both the CMTS and CM.

The most important key information is held by the CNMS. Key information is accumulated by a key-management server at the CATV head-end and by a key manager at the CM. Two cases are the saving of the master encryption key for a CM, and the case where a key is placed in an IC card, while another is set in a cable modem (CM). IC cards for BS broadcasting are to be mounted in the set-top boxes (STBs) of CATV systems, so the sharing of IC cards will be desirable for unified systems.

Fig. 5 is the state transition diagram for the CNMS of a CM. Here, the CMTS at the CATV head-end is already operating. This state transition diagram becomes effective when power is suppled to the CM.

The first transactions after the CNMS has started up is a check for the presence of an MEK in the CM and setting up of the RF-channel asssumptions [1] for the CM.

The CM's initial CNMS state is then processed. The coincidence between the MAC address and MEK on the CM and the values registered at the CATV head-end is checked; if they match, the process of KEK exchange/authentication proceeds.

At this time, the conditions for suspending CNMS operation include authentication failure and CNMS-start failure. When the setting-up of the RF-channel for a CM fails, the operation of that CM is stopped. When the TEK that has been encrypted by KEK after the successful distribution of the KEK is itself successfully distributed, encrypted communication using the TEK starts up. When the life-time of the KEK expires or TEK distribution is not possible, the system's state returns to the exchange of the KEK. CNMS operations stop if CNMS operation using the TEK is impossible even after several attempts to distribute the KEK and TEK. After the CNMS has been stopped, operations continue in a mode in which encryption is not employed.

3.2.1 CNMS Initialization

Let the period from start-up of the CNMS to operation of the CNMS with the TEK be the period of CNMS initialization. The CNMS and its initialization must be appropriate for a system based on asymmetrical modems. According to versions 1.0 and 1.1 of the DOCSIS specification, the initialization of the CM is as follows:

1) scannning and synchronization in the downstream direction;
2) obtaining the upstream parameters (UCD: upstream channel descriptor);
3) range-finding and automatic adjustments;
4) establishing the IP connections (DHCP: dynamic host-configuration protocol);
5) establishing the Time of Day;
6) transfer of operational parameters; and
7) registration for a CM.

There are three points at which the CNMS may be initialized; between steps 2) and 3) (case one), between steps 3) and 4) (case two), and after the registration step 7) (case three). The three cases and their good and bad points are summarized in table 2.

Table 2 CNMS initialization

Case	Techniques	Merits	Demerits
1	The MEK is used to encrypt the ranging information.	All of the information in the cable network is enciphered.	The prior registration of the CM's MAC address in the CMTS is indispensable (auto-registration is not possible)
2	The CNMS is set-up after ranging.	IP addresses are enciphered.	The timing of communications in equipment authentication is clearly known.
3	The CNMS is set-up after registration of the CM.	Initialization of the asymmetrical modems is easy.	The MAC and IP addresses that are in use become clear. The timing of communications in equipment authentication is clearly known.

Although per-customer tapping is clearly most difficult when the CNMS start-up is earliest, this approach places limits on the system's functions; e.g., in the first case, for the MEK to be used in encrypting the ranging demand from the CM, the MAC address and MEK of the CM have to already be in the CATV head-end. When users install new modems, they have to connect the modems to the CATV head-end at the MAC address level. Making a connection at the MAC address level is not easy for an amateur. On the other hand, in the second and third cases, customer authentication on the basis of the MEK is possible from the times of ranging and registration, respectively,

and automatic registration of the MAC address is possible. The second and third cases differ in whether or not someone who is tapping the network is able to read the IP addresses of the CMs. Moreover, the vendor ID of the modem and the MAC address of the CPE (customer-premise equipment), etc., are all clear when the CM is registered. After CNMS operations have commenced, the MAC address and IP address are encrypted, so the IP address is not distinguishable. The level of security is thus not strongly affected by the shift from the first to the second or third case. The problem of the timing with which the MEK is applied is thus solvable, to some extent, by having the MEK as the key for a strong form of encryption such as 3DES.

3.2.2 The Distribution of the TEK

All of the keys used by the CNMS, i.e., the MEK, KEK and TEK, are symmetric cipher keys. Of these keys, the MEK is mounted in an IC card or the CM and is delivered from the CATV head-end to the customer. Avoiding the use of a public key as the MEK obviates the authentication of a public key; the possession of the symmetric key itself is used for authentication. This simplifies the system. A further advantage of this approach is that delivery of the key should be comparatively easy in a fixed network such as a cable network.

New TEKs are frequently distributed but the periods between the distribution of KEKs are comparatively long. The TEK is changed at the end of a short and fixed period or on every transmission of data from the CM. This ensures that the encrypted MAC address is represented by different data on each transmission or in each of the short periods.

When the TEK is changed every time a fixed period elapses, the MAC address may be transmitted more than once during one period, i.e., as the same data. Let the fixed period be *tex* seconds. If n TEKs with attached index numbers are transmitted to each CM from the CMTS every time the keys are changed, the CM is able to randomly select one of the TEKs, attach its index number to a header, and transmit the result as encrypted data to the CMTS. In this case, a new set of TEKs is transmitted from the CMTS every $(n \times tex)$ seconds, and in response to this, the CM returns encrypted Ack data to CMTS. Although an asymmetrical cable modem is able to handle a downstream rate of 30 Mbps and thus has a large capacity, since the maximum upstream rate is about 10 Mbps, we need to look at whether or not the upstream flow of traffic is affected by TEK distribution. If N CM units are connected in one cell of a cable network and N is 1,000, the period between changes of the TEK *tex* is four seconds, the number of potential TEKs sent n is 4, and the Ack data *Dak* consists of 64 bytes, the upstream data rate for TEK exchange is

(*Dak* x 8) x*N* / (*n* x*tex*)=32 Kbps.

Although the upstream capacity will generally be much greater than 32 Kbps, the TEK-exchange period *tex* may be extended when sufficient capacity is not available.

3.3 System Comparison

Table 3 System comparison

Item	CNMS	BP
MAC address	Encrypted with the data.	Not encrypted.
IP address	Encrypted with the data.	Encrypted, but not during IP setup.
Authentication	Based on both the MAC address and MEK.	Based on the MAC address of the CM and the user's RSA secret key.
Collection of information on a specific customer	Extremely difficult.	Possible (however, the data is encrypted).

The specification of Baseline Privacy (BP) [2], which is managed by U.S. Cable Labs, includes the use of RSA public keys in the changing of the symmetric cipher key MEK for a CNMS, and the difference is making to solve with the application of a hash function to get the KEK for Baseline Privacy. However, in Baseline Privacy, encryption is not applied to the MAC addresses (DA and SA), and Baseline Privacy does not apply encryption when the IP addresses are set up. Someone who sees a MAC address at this stage is able to detect the terminal to which the information is being sent and its IP address. As is shown in table 3, a comparison of the results of applying the BP and the CNMS, the collection of information on a specific user is more difficult with the CNMS. Since several alterations of the TEK per day are sufficient for Baseline Privacy, the effect of these alterations on the upstream flow of traffic is negligible .

4. THE EXPERIMENT BY SIMULATION AND ITS RESULTS

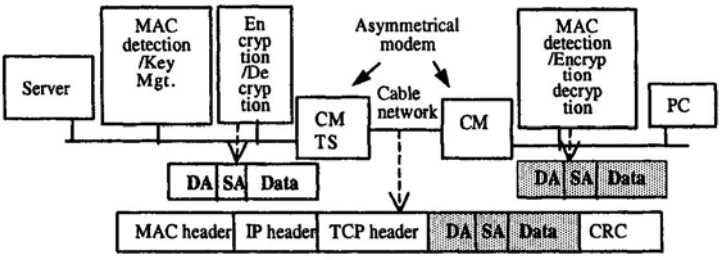

Figure 6. Block diagram of the experimental system

Although further experiments with the CNMS system will be necessary, including full testing on an actual CMTS at the CATV head-end and the CM units of customers, we have carried out an experiment by simulation at the application level. The simulation is of a limited environment.

4.1 Block Diagram of the Experimental System

The block diagram of the experimental system (Fig. 6) shows the encryption/decryption equipment and MAC-address-detection/key-management server that are added to the asymmetrical cable modem termination system at the CATV head-end and the MAC address-detection equipment, which includes a key manager, that is added to a customer's CM. The PC and the server make data, to which MAC addresses (DA and SA) are added, and in each case the whole is then encrypted. This encrypted data is then bi-directionally transmitted after a session has been established between the PC and the server. If both sets of encryption-decryption equipment correctly decrypt the encrypted data that has been sent, the CNMS is realizable.

4.2 Experimental Results

Logs of data that are the results of simulation with eight PC/CM sets, with TEK being altered every second, a downstream rate of 10 Mbps and an upstream rate of 2 Mbps, are given in Figs. 7 and 8. Each item of encryption/decryption equipment and the MAC-detection/key-management server ran on a 700-MHz CPU. The upper part of Fig. 7 shows the results of decryption of the MAC address in the log of data (lower lines) and the results of encryption (upper lines).

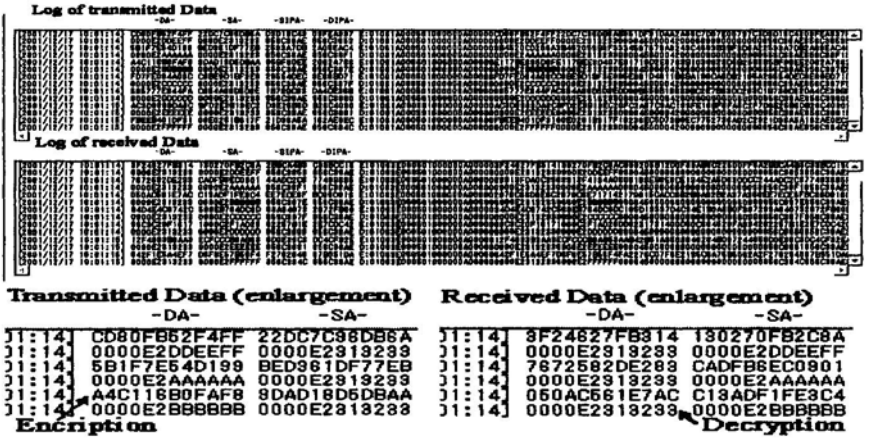

Figure 7. Logs of Data at the CATV head-end

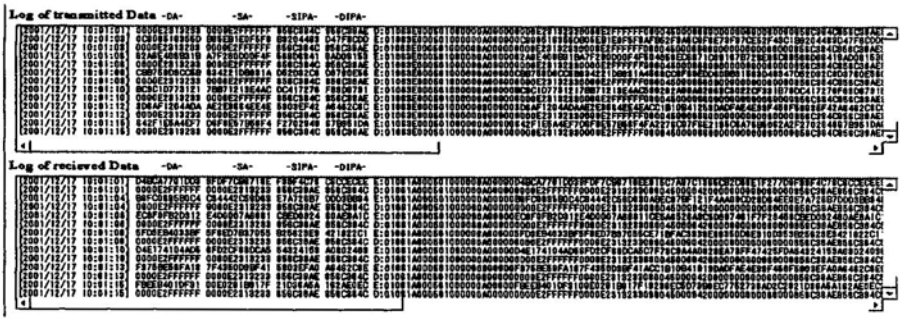

Figure 8. Logs of Data in a customer's PC

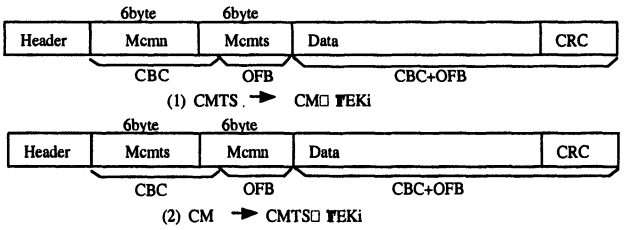

Figure 9. Method for encryption of MAC addresses

In Fig. 8, only the MAC address and IP address that correspond to the customer's CM have been obtained. The results of encryption for data transmitted to and received from a single CM at the same time are not the same, despite both transmissions occurring during a single TEK period (Fig. 7, lower part). Fig. 9 shows us why; the sequences with the MAC address of the CMTS, Mcmts, and the sequences with the MAC addresses Mcmn of the CM units are in opposite order in data transmitted and received by the CM, and the 8-byte block cipher MULTI2 includes 12 bytes of encrypted data in its CBC(cipher block chaining) and OFB(output feedback) modes. Sets of these 6-byte encryption results are shown in each of the enlarged displays of Fig. 7, and DA and SA head the corresponding columns. The same value is used for the initial vector in the cipher in CBC and OFB modes by all CMs and CMTS.

5. SYSTEM EVALUATION

The experiment result of Section 4 shows that the source and target of data are not identifiable in a system where the CNMS is applied. This provides security against tapping. To obtain data for a particular target, a

person who is tapping the network needs to be able to memorize all of the data in the 30-Mbps stream, and then to solve the encryption for each of the segments. It is difficult to continue memorizing all of the data and then encrypt it quickly enough for the result to be useful. Baseline Privacy (BP), on the other hand, allows the identification of data for individual target customers; a tapper is thus able to collect data for a given customer and then solve the corresponding encryption. Moreover, when the RAS secret key is also known, the tapper is able to decrypt all of the data. This also applies when IPSec [3], SSL [4], etc. is used with the cable network, i.e., as long as the MAC address is not included among the enciphered items. When the star topology is used to connect the central office with the individual customers, as is the case for telephone lines, it is impossible for a customer to obtain the data for others on the network without tapping the corresponding lines. When a wiretap is connected to a circuit, even if the addresses are encrypted, the person running the tap will be able to collect a specific customer's information. The installation of wiretaps by professional snoops and thieves always remains a possibility.

As an aside, no practically applicable security technique is able to handle attacks at level 1 of table 1. Although the quantum cipher makes it possible to detect interception, it is still difficult to prevent tapping. Even though attacks at potential level 3 require no special measures, a symmetrical modem allows a user to view common files that have been carelessly set up by other customers. The above points allow us to summarize robustness of security against tapping in table 4. We assume equal security for all ciphers.

Table 4 Robustness of security against tapping

Attack potential	Technique	Points
Level 1		
High ↑ Level2 ↓ Low	CNMS	All addresses are enciphered. Collecting a specific customer's information is very difficult.
	Telephone-line +IPSec, SSL, etc.	Wiretapping is an effective way to acquire data.
	BP, CATV+IPSec or SSL	The MAC address offers a good way to collect the information of specific customers.
Level 3	Asymmetrical modem	Tapping of downstream data is possible.
	Symmetrical modem	Tapping of downstream and upstream data is possible.

6. CONCLUSIONS

We have proposed the CNMS, where enciphering is in the MAC layer and thus applied to the MAC address, as a way to improve the security of cable networks. The CNMS destroys the value of tapping, which is the weak point

of cable networks, and so it is more secure than other security systems. We confirmed the promise of the CNMS in an experiment by simulation of an asymmetrical-modems-based cable network. We confirmed that the system provides a practicable solution. A standard is indispensable to widespread application of the CNMS. We thus need to look into the optimization of the cipher protocols, etc.

REFERENCES

[1] DOCSIS (Data-over-Cable System Interface Specifications): "Radio Frequency Interface Specification", SP-RFI-106-010829, August 2001

[2] DOCSIS (Data-Over-Cable System Interface Specifications): "Baseline Privacy Interface Specification", August 2001

[3] RFC2401 "Security Architecture for the Internet Protocol", November 1998

[4] RFC2246 "The TSL Protocol Version 1.0", January 1999