광대역통신망을 위한 보안 프레임 구조 분석

김정태*

Analyses of Security Frame Structture for Broadband Communication

Jung-Tae Kim*

요 약

인터넷을 이용한 정보가 모든 정보 전달의 기본이 되고 있다. 따라서 이러한 정보 전달의 보호를 위한 정보보호 산업이 급성장하게 되었다. 따라서, 본 논문에서는 유비쿼터스 환경 하에서의 각 가정의 홈 네트워크 구성을 위한 외부의 망을 고속화 할 때 필요한 보안적인 측면의 방법에 대해서 제시하고자 한다. 본 논문에서 제시하고자 하는 내용은 암호학적으로 안전한 광통신 기반의 네트워크의 구성과 이를 실현하기 위해서 요구되어지는 다양한 고려사항 등을 분석하여 차세대의 유비쿼터스 환경하에서의 정보보호 시스템 구축에 도움이 되고자 한다.

ABSTRACT

Information transfer technology using Internet is basic means today. Therefore, we have to consider the information through internet. The main key is Information security against attacker. We have proposed the method employing security mechanism under ubiquitous environment. To realize the Information security for optical communication, we need requirement for a variety of consideration and propose the method..

키워드

광통신, 광대역통신, 정보보호

Ⅰ. INTRODUCTION

Video on deman, broadcasting, and high-speed transfer require a wideband communication. To reduce the high costs of laying individual cables for each user and install costly optical terminals to both ends of them, passive optical networks(PON) are being developed in the recent years, in which the longer part of the network is common to and shared by many terminals, while only networks are used in combination with new fiber optic cables constituting hybrid fiber coax(HFC) networks. All these networks work in ATM mode. The data arriving at the central station, which are destined for its terminals, are time pultiplexed to form a single bit stream which is

broadcast to all terminals. Each terminals selects the data destined to it, either by the aid of the identification field contained in the overhead of the downstream cell, or, most usually, by the Virtual Connection Identifier(VCI) field contained in the ATM cell. The configuration is shown in figure 1.

*목원대학교 공과대학 정보전자영상공학부

접수일자 : 2004. 10. 29

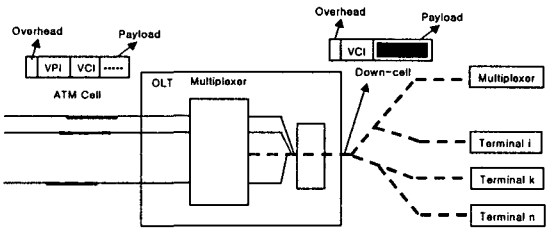

Figure 1. Time multiplexing of downstream cells

II. CONVENTIONAL ENCRYPTION

Conventional encryption is generally carried out by using some ciphering code according to which every bit of the original text is replaced by another bit, so that the resulting text has no meaning to any one except for the user to whom it is destined, who has the proper code to encrypt it and recover the original text. Several methods for encryption have been developed and proposed using both block cipher and stream cipher. Most problems in the conventional encryption arise exactly in common method. More problems arise when we wish to encrypt also the headers of the downstream cells in order to aviod speculation on ones traffic parameters. If we encrypt, for example, the field of the downstream cell which contains the identification number of the addressed terminal, or the virtual Connection Identifier(VCI) field of the ATM cell., then all terminals should have to decrypt these fields in all received cells in order to find out which cells are addressed to them. This poses a very heavy and time consuming work on the terminals, which, even of it would be possible to be executed in the necessary speed, leads to expensive terminals.

So, with conventional encryption, we usually encrypted only the payload of the downstream cells and cannot avoid speculation on the traffic data of the users. The encryption can be done, either in each incoming stream before the time mu;tiplexing as shown in fufure, or in the common downstream, after the time multplexing. In the first case we need many encryption machines working at a relative lower speed which can be achieved. In the second case we need one encryption machine, which work in very high speed, which do not seem likely that will be feasible.

III. THE PROPOSED SCHEME

The proposed method utilizes the same characteristics of the network architecture that causes the problem, that is the broadcasting nature of the downstream data, in order to secure the lost privacy and individuality. Multiplexing is usually done in cell level, that is each ATM cell contains data of one connection only, and, by means of the VCI number contained in the corresponding field of the header, it is destined to the terminal serving that connection. Sometimes however for reason of maintaining low delay or delay variation it is necessary that multiplexing is done in byte level, in which case composite cells are formed with bytes from more than one connection destined for more than one users. In the later case the termainal understnads which bytes of the cell are destined to it either by information contained in front of the bytes, or by the fix places within the ATM cells in which the bytes destined to it are placed. The proposed method uses always composite cells for the connections to be encrypted, but the bits in the cells are multiplexed in a different random way for every connection, which we call multiplexing pattern, and this pattern is known only to the central station and to the terminal serving that connection. This pattern plays the role of the session key of the conventional encryption and is changed in every new connection.

All downstream cells, which usually have 54 bytes, have a characteristic bit in their header. If the bit is 1 then the cell is a composite "encrypted" cell. If the bit is 0 the cell is not encrypted cells have their ID or VCI number the encrypted cells have an identification number ranging from 0 to (Tn-1). The number Tn is the basic period, further called basic module, of the downstream for encrypted cells and is depended on the capacity of the downstream data flow and

desired granularity of the services offered.

Here we will describe the case of a super PON with a downstream capacity of 2.54Gbps. For reasons which will be understood later, Tn has been chosen to be 211. So the same identification number of a cell will appear 211 encrypted cells. Given that every downstream cell has 200 payload bits, the basic module contains about 400*211 = 8192000 bits of information. Every bit place of the payloads of the downstream cells is enumerated from 1 to 400. So with 9 bits we can enumerate all the places of a cell and the last 9 to the place inside the cell.

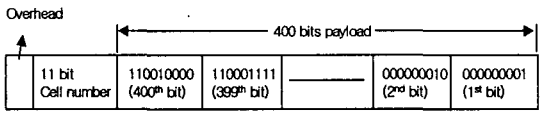

Figure 2. Enumeration of the bit places inside the downstream cell

When a new 16 Kbps connection is to established the cenral station selects randomly 8 out of the 819200 possible places for that connection, taking care that they are free from other conncetion. This constrain do not influence the randomness of the choice because the occupied places have also been chosen randomly. The selected places are the multiplexing pattern of the connection. For the description of the pattern we simply write down, one directly after the other, the eight numbers indicating the places where the bits of that connection are put. So for the description of the whole pattern we need 8 x 20 = 160bits. We need also 3 extr bits to indicate that this pattern refers to the basic module.

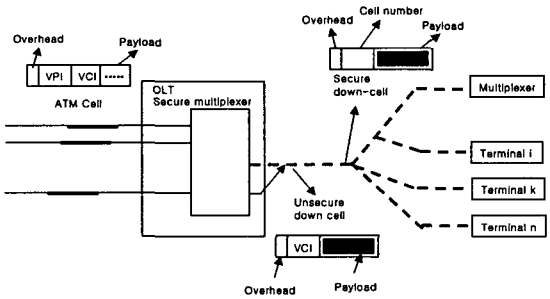

Figure 3. The proposed scheme of secure communication of the downloadstream data

The multiplexing pattern, which play the role of the session key of the conventional encryption, is communicated to the corresponding terminal through one of the OAM (Operation and Maintenance) cells interchanged between headed and terminal station during the establishment of the connection. The payload of the OAM cell is encrypted by one of the public key encryption method. The only thing that the corresponding terminal has to do in order to reassembke the bits of the connection is to select and place one after the other the bits contained in the places indicated by the multiplexing pattern, in the same order as the places are written in the later. When a connection is terminated the places are free again to be ised for the formation of multiplexing patterns for other connections. The connections that do not need protection are put in uncrypted cells, which intervene between the encrypted ones and are not counted for the multiplexing pattern. The methos is presented in figure 3.

When a 64Kbps connection is established, which needs 32 bits per basic period, it is not necessary to use a pattern extended in the whole period. Instead of it we use a subperiod consisting of the first 29 cells of the basic module, in which we choose a pattern of 8 bits. This pattern is repeated 4 times in the basic module. For the description of each place of this subperiod we need 18 bits(9 for the cells inside the subperiod and 9 for the places insides the cells). We need also some bits to indicated that we use a s subperiod consisting of the 1/4 of the basic period. For 1 128Kbps connection, the same 1/4 subperiod is used. In this case we need a 16 bit pattern, which requires 291 bits for description and has about 1084 possible multiplexing patterns. For a 256Kbps connection we use a 1/8 sub period with 16 bit pattern, which has about 1080 possible multiplexing patterns. For connections of 512, 1024 and 2048 Kbps we use correspondingly 1/16, 1/32 and 1/64 sub periods, always with a 16 bit pattern, which have about 1075, 1070 and 1060 possible multiplexing patterns. For their description we need correspondingly 275, 259 and 243 bits. For intermediate values of bitrates we use either the longer subperiod with more bits pattern, or the shorter subperiod with fewer bits per

pattern. The scope is always to have the more possible combinations, while for the description of the multiplexing pattern and the rest information which will be communicated to the terminal during the connection, we will not need more than 386 bits which is the payload of one ATM cell.

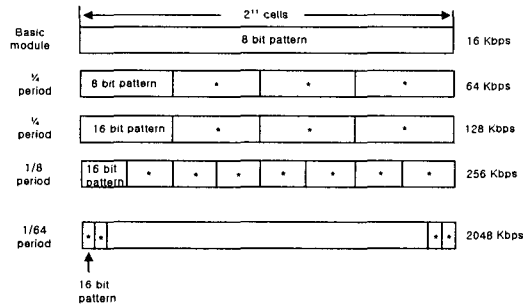

Figure 4. Overview of the different multiplexing patterns

This number is also smaller than the numbers used in the public key exchange procedures, so that the initial notification of the multiplexing pattern to the terminal poses no difficulty. For largerer than 2 Mbps bitrates, we use 1/64 sub period with up to 24 bits per pattern, which corresponds to a capacity of 3Mbps. For still higher bitrates we can use an 1/128 sub-period, but it seems very unlikely that such bitrates will be needed, since with modern compression methods 2 Mbps are sufficient even for video on demand services.

IV. FUTURE WORK

All optical network is network where the user network interface is optical and the data does not undergo optical-to-electrical conversion within the network. All optical network is attractive because they promise very high rates, flexible switching, and broad application support. The emergence of these networks coincides with a burgeoning use of networked information for education, commerce, health care, national defense, and many other endeavors that promise continued growth for decades. Assured access to these networks, in a private and reliable manner and with appropriate service guarantees, is clearly very important and has motivated for the security of all optical network.

V. CONCLUSIONS

In some kind of networks such as PON and HFC networks, the inforamtion from the central station to the terminals is broadcast to all of them. Under these conditions privacy and confidentiality do not exist. The usual way to overcome this drawback is conventional encryption of the data between headend and terminals. The proposed scheme is to use different multiplexing patterns for each connection so that each terminal can demultiplex only its own data. The proposed method is suited for the high speed data of the PON networks and maybe preferable to conventional encryption.

References

[1] J.Koulouris, et al., "Securing confidentiality in PON and HFC networks", SPIE 1998, V.3408, pp.148-158

[2] Muriel Medard, "Security issues in All optical Networks", IEEE Network, May, 1997, pp.42-43

[3] I.P. Kaminow, et, al, "A Wideband All-optical WDM network", IEEE J. Sel, Areas Comm., V.14, N.15m Jun2 1996

저자소개

김정태(Jung-Tae Kim)

Received his B.S degree in Electronic Engineering from Yeungnam University in 1989 and M.S. and Ph.d. degree in Electrical and Electronic Engineering from the Yonsei University in 1991 and 2003.

From 1991 to 1996, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 2002, he joined the department of Information Electronic & Imaging Engineering, Mokwon University, where he is presently a processor. His interest is in the area of Information security.