초고속정보통신망을 위한 광 네트워크에서의 보안 모델 해석

김정태

목원대학교

Security Issues in All-optical networks for High-speed Information Communication

Jung-Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

Abstract

All-optical networks are emerging as a promising technology for per second class communication. However, they are intrinsically different from electro-optical networks, particularly because they do not regenerate signals in the networks. The characteristics of all-optical network components and architectures manifest and still unstudied security vulnerabilities but also offer a new array of possible countermeasures. In this paper, we have analysed the security issue to protect against intrusion.

Ⅰ. Introduction

All optical network(AON) is a network where the user network interface is optical and the data does not undergo optical to electrical conversion within the network. AONs are attractive because they promise very high rates, flexcible switching, and broad application support. Currently, optical transmission links supporting 30 - 40 Gbps are commercially available, 100Gbps products have been announced, and terabit-per-second AONs have been demonstrated to tap economically this large capacity because fiber optic transmission technology is progressing faster than electronic switching technology, and because optical switching technology is maturing to the point where it may become the economical choice in certain applications. Research testbeds have demonstrated basic AON functionally with transmission rates of over 100 Gbps in local and metropolitian area networks. Access networks represent thje most cost-sensitive part of the communication infrastructure since they cover the links of the customers to the network which are unique for each domestic site and must be directly or indirectly paid by the corresponding customer. Low traffic intensities and low sharing of infrastructure lead to slow return on investment making the undertaking of an upgrade to higher rates a risky project. For these reasons, shared architectures such as Passive Optical Networks(PONs) in combination with the Asynchronous Transfer Mode(ATM) are considered one of the most promising solutions for the introduction of broadband services to residential users. The trunk and the main branches of the network consists of optical fibers in common use. Only the last drop is dedicated. Statistical multiplexing of ATM cells effected with the help of the Medium Access Contol(MAC) protocol can dynamically adjust bandwidth distribution

among many traffic streams based on momentary needs, and so lower the per user cost of the infrastructure.

Ⅱ. Typical PON system structure

The main feature of a PON architecture is its tree topology with a central point at the root of the tree through which all traffic has to pass. Optical splitters divide the signal into N equal copies in the downstream direction whereas they multiplex the upstream transmission into a signal stream directed to the local switch. TDMA multiplexing of cells is adopted since it has emerged as the most effective method. For the proper operation of the TDMA method, the cells transmitted upstream must combine in a way creating a train of cells without catastrophic overlaps and with a minimal and controlled intercell spacing. In a Passive Optical system, multiple optical network units provided in the subscriber's homes and one Optical Subscriber Unit(OSU) provided in the optical line terminals are connected point to point multiple point through an optical splitter. The OSU can be shared by multiple subscribers and an economical optical access system can be implemented. A method using time compression multiplexing/time division multiple access was proposed.

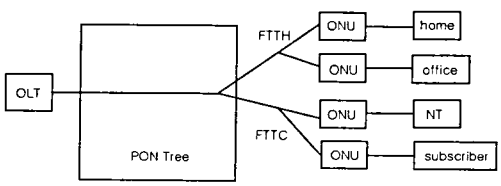


Fig 1. Typical PON Architecture

III. Requirement of service and threats

The following features and conditions of the PDS system must be considered when determining the encryption method.

- The upstream communication is unicast and the downstream communication is broadcast
- Bit errors may occur in the communication process due to thermal noise and external noise
- Fixed bits pattern or signal-free intervals exist in the upstream and downstream signals
- A small size and economy are required.

The security measures required in a passive optical networks are as follows.

- Confidentiality of user data
- Confidentiality of signaling data
- Authentication of user/user device to network
- Authentication of network to user/user device
- Integrity of user data
- Integrity of signaling information

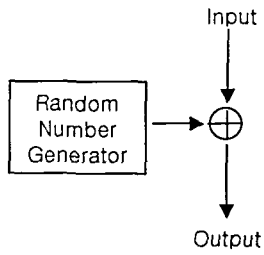
IV. The proposed Encryption Method

Encryption has the important role of turning the inherent broadcast downstream architecture into a point-to-point one. Thus although on the physical level all information still reaches all customers, each one should be able to decrypt and understand only the cells addressed to him. In contrast, the upstream direction is much less vulnerable. The only concern arises from the reflections of the upstream signals on the optical splitters. These

reflections are detectable but most probably not readable at the customer premises. The proposed solution could be applied to both directions in the event tht the reflections prove to be a security risk.
Encryption methods are classified into two types. block ciphers and stream ciphers. A block cipher is an encryption method that handles data in units of several bytes to several dozen bytes, whereas a stream cipher can encrypt units of 1 bit to several bits. In a communication process, since a 1 bit error spreads to all of the bits as the encryption process unit during ciphertext decryption when 1 bit of the received signal has been corrupted by noise, stream ciphers can lessen the effect on bit errors more than block ciphers can. And since the size of the encryption circuit is smaller for the stream cipher that handles less data, a stream cipher was used as the encryption method that satisfies requirements. Of the stream ciphers, vernam cipher has been proven to be a perfect cipher cipher. However, the following two problems occur when the vernam cipher is applied to the proposed method.

- Implementation is not possible because a sequence of true random numbers having the same length as the plaintext to be encrypted is required.
- when the entire downstream signal is a logical "0", the information of pseudorandom number required in the decryption is leaked.

Figure 3 shows the structure of the proposed method and the frame format of the PDS system. The upstream signal is sent to the OSU after randomization by scrambling in the ONU. The OSU uses this upstream signal to generate the pseudonrandom number and encrypts the downstream signal in the encryption circuit. Similarly, the ONU generates the pseudorandom number and decrypts the downstream signal.



Fog 2. Principle of Vernam cipher

Pseudorandom numbers are generated for each user channel by using each upstream user channel and used in encryption and decryption in the corresponding downstream user channel. For instance, even if the UC has no signal, or the widths of UC and DC differ, encryption becomes possible as described later. The basis of this method is the unpredictability of the upstream signal which is not known by the other subscribers. When the attacker uses the ONU belonging to the same OSU as the ONU targets for attack, the contents of the call sent from the targeted ONU can be found by calling the targeted ONU. Therefore, not only upstream data sent by the user, but also the upstream signals for the maintenance and monitoring terminated by the ONU and the OSU are required in pseudorandom number generation. By adopting a structure having a feedback loop as the upstream scrambler in the proposed method shown in fig3, the signals for the maintenance and monitoring to be sent with the upstream data are used in pseudorandom number generation by feedback and taking the

exclusive-or with the user data. A a result, encryption becomes possible because a different pseudorandom number sequence is generated by the values of the signals for maintenance and monitoring even when all of the upstream user data become logical "0" temporarily.

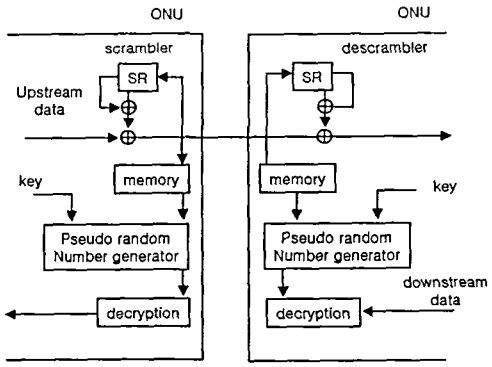


Fig 3. A Circuit for Encryption and Decryption

V. Element technology of security system

It is a popular misconception that security is synonymous with encryption. In many cases, confidentiality via encryption is that the least important element of a security solution. Network security involves a number of different elements:

1. Data origin authentication
2. Command authorization
3. Message integrity protection
4. Message replay prevention
5. Data confidentiality
6. Key distribution
7. Trust versus trustworthiness

VI. Conclusions

Sharing the OLT and the feeder fiber by means of PONs or reduces the per customer cost of access to broadband services but at the same time privacy is compromised. To rectify this problem resort to cell level encryption is adopted. Because of the high speed, hardware based solutions must be chosen. A stream cipher solution based on the summation generator is found suitable for the purpose must be chosen. A stream cipher solution based on the summation generator is found suitable for the purpose in combination with a public key management scheme. The proposed method has the some features. First, the unpredictability of the pseudorandom number was improved by using a method for pseudornadom number generation that used the upstream signal as the encryption key. Second, leaking of the pseudorandom number information can be prevented during the signal-free period.

References

[1] Kumozaki K, "Functional structure of the fibe-optic passive double star system", IEICE Trans Commun 1992, E75, pp.832-840

[2] Okamoto E, "A proposal for nonlinear random generation method", 1986, IEICE sociry conference, n.1432, 1986

[3] J. Gait, "A new non linear pseudornadom number generator", IEEE Tran. on Software Engineering, SE.3, no.pp.353-359, 1992

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

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