韓國 OA學會 論文誌
第3卷 第3號, 1998. 10.

98-3-3-3-1

ATM망에서의 보안과 인증

임 청 규*

A Security and Authentification for ATM Network

Chung-Kyu Lim*

요 약

본 논문은 초고속통신망(ATM) 등장으로 다양한 서비스가 가능하나 정보 메시지의 위협 및 취약에 대한 대비가 부족하다. 본 논문은 ATM망에서의 메시지 보안과 인증기법을 제시한다. ATM망의 AAL 과 ATM계층간의 보안계층설정을 위한 ATM프로토콜의 서비스 옵션이 응용된다. 제안된 보안과 인증 기법은 AAL과 ATM계층간 호 설정 과정에서 신호 프로토콜 형태로 제시된다.

Abstract

This paper presents a security and authentification scheme against unauthorized disclose and attack in ATM(Asynchronous Transmission Method) with various service. Four various options to place security layer between the AAL and ATM layers is discussed. The suggested security and authentification can be integrated with the call setup procedures of ATM.

* 정인대학 사무자동화과 전임강사
논문접수:98.8.18. 심사완료:98.10.23.

I. Introduction

A broadband multimedia networks such as broadband integrated services digital network(BISDN), will be required to carry the traffic by a wide range of services. These services will have diverse traffic flow characteries and performance requirements.

The asynchronous transfer mode(ATM) is currently being considered by ITU-TS (International Telecommunication UnionTelecommunication Standardization Sector) as the prefered transfer method for the BISDN. ATM will provide the means to transport, at broadband rates, the traffic generated by a wide range of multimedia services. Multimedia services require some combination of text, image, voice, and video storage and communication [1-4].

A basic attraction of ATM networks is their ability to carry different types of information, namely voice data and video from one user to another over a local or a wide area. Therefore, it is clear that securing these different types of information over high speed ATM networks is becoming increasing critical [5-7].

This paper addresses the security and authentification issues that one needs to consider in developing secure ATM networks. The authentification is the first step in establishing secure communications between two systems.

Due to threats of spoofing, this is required before any other security mechanism such as key exchange or encryption may be deployed. Current uses of authentificated exchanges include SNMP and OSPF. Methods of authentification include the use of symmetric algorithms such as DES , where the two parties must first share a secret key, or public key algorithms including RSA, where each node must only know the other's public key. For the authentification of two end systems with verified identities, EBCDIC-coded cryptosystem with key directory is remarked.

The paper is organized as follows. Section 2 gives a brief overview of security Threats and services for ATM. Protocol Reference Model (PRM). Section 3 discusses the options for the placement of security services with the ATM PRM. Section 4 suggests the model of the cryptosytem and authentification model for data confidentiality and integrity between the AAL and ATM the option.

II. Security Threats and Services

2.1 Security Threats

ATM networks are able to carry some combination message of text, image, voice and video which can be of a private and sensitive nature. There, like any other networks, ATM networks are susceptible to the following threats.

· Masquerade

Masquerade occurs when the message entity successfully pretends to be a different entity and can take place in a number of ways. An unauthorized end-user amy imperonate authorized user to gain unauthorized access to data and facilities.

· Message sequencing

Message sequencing threats occur when part or all of a message is repeated, time-shifted, or reordered. This can be used to exploit the authentification information in a valid message and resequence or time-shift valid message.

· Modification of information

Information for an intended recipient, routing information, and other management data may be lost or modified without detection. This could occur to any aspect of the message e.g., its labeling, contents, attributes, recipient, or originator.

· Denial of Service

Denial of service occurs when an message fails to perform its function or prevents other entities from performing their functions. This may be a denial of access, a denial of communications, a deliberate suppression of message to a particular recipient.

· Repudiation

Repudiation can occurs when an end-user or the other user may later deny submitting, receiving, or originating a message. Repudiation threats include the following denial of origin, denial of submission, denial of delivery.

· Leakage of information

Information amy be acquired by an unauthorized party by monitoring transmissions, by unauthorized access to information stored in any message entity, or by masquerade.

· Other threats

A number of threats may exit that relate to security labeling, e.g., routing through a node that cannot be trusted with information of particular value, or when systems use different labeling policies. Threats may exit to the enforcement of a security policy based on logical separation using security labels.

2.2 Security Services

· Information Confidentiality

This service protects information against discloser between a sender and a receiver. There are some high speed encryption devices that are available.

· Information Integrity Service

This service protects information against modification between a sender and a receiver.

· Authentification Services

This services provide a recipient with assurance that a message came from the claimed originator.

· Non-repudiation Services

This services provides a recipient with irrefutable proof of the origin of an information and the originator of an information with irrefutable proof.

Ⅲ. ATM Protocol Reference Model and Security Layers

3.1 ATM protocol reference model

The primary layers of the ATM protocol reference model are the physical layer, the ATM layer where the cell structure occurs, and the ATM Adaptation layer(AAL) that provides support for higher layer services such as circuit emulation, frame relay, and SMDS. The physical layer corresponds to OSI reference model layer 1, layer 2, and higher layer correspond to OSI layer 3 and above.

The ATM model contains three planes. The

user plane(U-plane) is responsible for providing user information transfer, flow control, and recovery operations. The control plane(C-plane) is responsible for setting up a network connection and management the connections. It is also responsible for connection release. The control plane is not needed for permanent virtual circuits(PVCs).

The management plane (M-plane) has two functions: plane management and layer management. Plane management has no layered structure. It is responsible for coordination of all the planes. Layer management is responsible for managing the entities in the layers and performing operation, administration, and maintain services(OAM).

3.2 Security Layer

The placements of he security mechanism between the ATM and the AAL layers makers them transparent to the adjacent layers. In this case, the security mechanism operate on the fixed size SAR-PDUs. The entire cell can be encrypted, as the header is added by the ATM layer below. Techniques such as feedback chaining techniques and stream ciphers can be used which do not cause data expansion. In this paper, the EBCDIC coded encryption can be used for data confidentiality.

Ⅳ. The Cryptosystem and Authentification Model

4.1 The Cryptosystem Model

The model of the cryptosystem based on the security layer in section 3.2 is depicted in Fig. 1. This system applies a secret key. Both sender and receiver are secret. The key K used as the solution of encryption and decryption depends upon the condition of the generated.

The encryption algorithm with the key transforms the digital signal into ciphertext of an unintelligence form. The decryption algorithm with the key transforms the ciphertext of an unintelligence form into the digital signal.

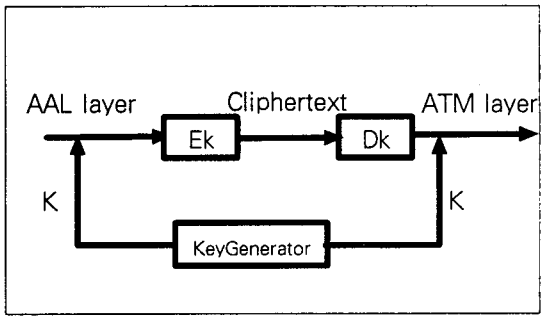

Fig. 1.

4.2. Data Authentification

The key kept in a key directory sender A in AAL layer and receiver B in ATM layer is sharing. The KD is responsible for maintaining, updating, and distributing the key used in the transmission network. Figure 2 and Figure 3 describes the authentification diagram, and procedure, respectively. In the first message of the protocol, the initiating partner, sender A, asks a KD for the key RQA, along with the current time T1. Knowing KE, a user can decipher the cryptogram and extract an authentic key KE, a copy of the request RQA, and the time T2. Now, having the public key KB, A send B a cryptogram DKA[EKB(M, RQA, T2)].

Receiver B ask the KD for the key KA along with the current time T2(4). In response, the KD transmit to B the cryptogram EKA[DKA [EKB(M, RQA, T2)], RQ3, T3]. To complete mutual authentification, the verifier B responds in (6) with the cryptogram DKB[EKA[DKA,

EKB(M, RQA, T2)], RQ3, T3], T4], along with the time T4. If the cryptogram and the original match, it is assumed to be authentic.

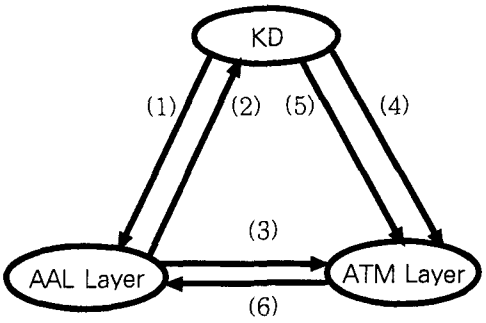

Fig. 2.

(1) AAL Layer ---> (RQA,T1) ——> KD
(2) AAL Layer <- EKB(M, RQA, T1) <— KD
(3) AAL Layer ——> DKA[EKB
(M, RQA, T2)] --> ATM Layer
(4) ATM Layer ---> (RQB, T2)——> KD
(5) ATM Layer <— EKA(DKA [EKB(M, RQA, T2)], RQ3, T3) <— KD
(6) AAL Layer <— DKB(EKA (DKA EKB (M, RQA, T4)], RQ3, T4), T4) <— ATM Layer

V. Conclusion

We suggested a secure cryptosystem model and authentification model for ATM networks. This model provides four kinds of security services, EBCDIC coded cryptosystem, message authentification, data confidentiality, and data integrity. We need simulation model to implement the above suggested model and to analyze the numerical complexity. This system provides secure services protecting the security threats and authentification services. This paper proposes a model of secure cryptosystem model and authentification.

References

[1] Uyless Black, "ATM:Foundation for Broand Betworks", Prentice Hall Serices, inc., 1995.
[2] David E. McDysan and Darren L. Spohn, "ATM:theory and Application", McGraw-Hill Series inc., 1994.
[3] J M Pitts and J A Schormans, "Introduction to ATM Design and Performance", John Wilwy&Sons inc., 1996.
[4] "ATM solutions for enterprise internetworking", Addison -Wesley inc., 1996.
[5] Steven D., Hillary N. and Byrd G., "Secure communications in ATM networks", Vol 38, No.2, Communications of the ACM, 1995.
[6] Chuang S.C., "Securing ATM networks", Third ACM conference on computer and communication security, New Delhi, India, 1996
[7] 박정현, "초고속 정보통신망에서의 안정성 대책방향과 정부역활", 정보처리학회지, pp.24-32, 3, 1997.

저자소개

임청규