SECRECY AND PRIVACY IN A LOCAL AREA NETWORK ENVIRONMENT

by

Gordon B. Agnew
Department of Electrical Engineering
University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1

Abstract

In recent years, much effort has gone into the development of high bandwidth communication networks for use over relatively short (local) distances, e.g. an office, an industrial complex, a research laboratory, etc.. The high bandwidth of these networks allows many of the services now requiring separate networks such as facsimile, digitized voice, file transfer and interactive terminal data, to be integrated into a common transmission facility. Manufacturers are currently developing products which conform to the recently established IEEE 802 standard for Local Area Networks (LANs). This standard is based on the concept of a layered, "peer entity" communication protocol put forth in the International Standards Organization's (ISO) seven layer model for Open Systems Interconnection (OSI).

In this paper we define the notions of secrecy and privacy as they relate to a LAN environment and the various services a network is required to provide such as data integrity, authentication and digital signature services. We also describe the cost-benefit tradeoff involved in attaining various levels of privacy and secrecy.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 349-363, 1985.

1.1 Introduction

This paper will be presented in two parts; the first part is a general description of the secrecy and privacy requirements in a local area network environment. In the second part of the paper we present some observations and proposed methods for integrating secrecy and privacy into established network protocols.

In the past few years, much research and development has been concentrated in the area of local communication networks. In general, local area communication networks (LANs) provide a multiple access environment over a relatively small geographical area such as a room, building or group of buildings with maximum network lengths of a few kilometers. An introduction to local area networks and there applications can be found in [1]. The main characteristics of a LAN can be summarized as follows:

1. Topology - ring, bus or star are the most popular configurations (see Fig. 1)
2. Transmission medium and technology - there are two popular methods
   - coaxial cable - baseband or RF modulated transmissions
   - fibre optic
3. Media Access Protocol- there are two broad classes of media access protocols - contention (random access) protocols and non-contention protocols
4. Communication protocols and type of services provided by the network (i.e. unacknowledged connectionless services, connection oriented services[1]).

LANs are finding increasing applications in research, industrial and office environments where the trend is towards the integration of many services such as digitized voice, interactive terminal data, facsimile transfer, file transfer and electronic mail into a single common communications facility linking all users. A characteristic which is common to all LANs is the ability to establish a connection between any pair of users (transceivers). This is usually accomplished by broadcast techniques where the message is transmitted on the network along with source and destination information in such a way that all of the transactions on the network can be heard by every network transceiver. In addition to the study of various applications, work is proceeding on the development of communications protocols for LANs.

1.2 The Open System Interconnection Model

The International Organization for Standardization (ISO) has proposed a model for communication protocols in networks called the Open Systems Interconnection (OSI) model and is currently being used as a basis for the IEEE Project 802 standard for LANs [3]. The OSI model, shown in Fig. 2, defines seven layers of complementing protocols where communication is defined as taking place between equivalent or peer entities at each user site. To facilitate this, the upper layers are built on the services of the lower layers (as well as adding value to the services) in such a manner as to isolate the user from the physical operation of the network. The n-layer services of a layer are the capabilities it offers to n-layer users. Thus, at the higher layers, the user is not aware of, or concerned with, the operation of the network as this becomes transparent. A summary of the OSI model can be found in [2].

---

[1] These terms are consistent with Type I and Type II Logical Link Control (LLC) services of IEEE 802.2.

1.3 IEEE Project 802

The IEEE 802 standard is actually a family of standards 802.1 through 802.6 which deal with the physical and data link layers of the OSI model. Fig. 3 shows the relationship between the IEEE Project 802 standard and the ISO model.

Standard 802.1 is used to describe the relationship between these standards and the OSI model. Due to the diversity of media-access methods and transmission technology (as was described previously), a number of standards were required to cover the physical and data link layers. In the 802 standard, the data link layer is split into two sublayers, a common Logical Link Control sublayer (LLC) and a Media Access Control (MAC) sublayer which is contoured to the requirements of the various types of LANs i.e.:

802.3 standard for CSMA/CD bus networks
802.4 standard for token-passing bus networks
802.5 standard for token-passing ring networks
802.6 standard for metropolitan area networks (MANs).

This structure allows a common interface at the LLC sublayer and information (Protocol Data Units) passing into and out of the LLC from above (Network Layer) or from below (MAC sublayer), are standardized.

A detailed description of these standards is beyond the scope of this report (see [4]-[6]) but we will describe a few of the basic principles. As mentioned previously, all layers are built on the services they provide or use. The general format of messages to/from the various layers is shown in Fig. 4.

Messages may be of three generic types:

i)Request - a primitive for requesting n-layer services from a n-layer user

ii)Indication - a primitive used to indicate to a n-layer user of an internal n-layer event which may be significant (e.g. a remote service request)

iii)Confirm - a primitive which conveys to a n-layer user the results of a previous request for n-layer service

All communication and information passing is performed using this type of hierarchical structure.

The LLC layer supplies two types of message exchange services: i)Type I, Unacknowledged Connectionless Service and ii)Type II, Connection Oriented Service. In Unacknowledged Connectionless service, network layer entities exchange Link Service Data Units (LSDUs) without establishing a data link level connection. In Connection Oriented service, LLC provides the means for establishing, using, resetting and terminating data link layer connections along with data link layer sequencing, flow control and error recovery procedures. Thus, the message transfer services can be loosely coupled ("datagram") or tightly coupled ("virtual circuit") type connections.

1.4 The Problem

The increased use of digital communications for business transactions also increases the need for secrecy and privacy. Unfortunately, the two requirements are sometimes contradictory. On one hand, we require access to a wide variety of services yet, we may wish to keep the information exchanged secret. The various types of traffic on the network will have different characteristics and requirements such as delay, buffer space and priority. In addition, different types of traffic will have different security requirements. For instance, in an industrial environment, top level memos may require complete secrecy. In the banking environment, more emphasis is placed on the authentication of a transaction than on its secrecy. In the most basic time-

sharing systems, the operating system must ensure only legitimate users are allowed access. For digitized voice, most people are content with the level of privacy provided by an unencoded analog telephone connection; their only real concern is that a conversation does not allow "party-line" interception, that is, no casual listener can overhear their conversation, thus, the normal level of privacy for voice is minimal. Data bases tend to be available to all users but clearly, steps must be taken to prevent unauthorized additions or deletions. If we consider the concept of an electronic mail service, one would envisage a central mail server which would act as a temporary depository for messages which could not be immediately delivered. This type of service presents a difficult problem in that messages must be authenticated when they are placed in the service, they must be protected from unauthorized disclosure, addition, modification and deletion while in the mail server and they must be delivered in a manner which will preserve the privacy of the message (this tends to be a more complex problem than a secure database system).

Our objective in this paper is to outline some possible methods by which secrecy, privacy, and authentication techniques can be incorporated into a hierarchically structured network using already established protocols as a base. An example of the type of network where these methods may be applied is the Waterloo Experimental Local NETwork (WELNET) which is classified as a non-contention broadcast network which conforms to the IEEE 802.2 standard for Logical Link Control (LLC) (see [7]).

In the IEEE 802 standard and OSI model a (N-1) layer may supply services to more than one N layer entity. The (N-1) layer and N layer communicate through Service Access Points (SAPs) which are addressable points in each layer. When a message is generated, the source N layer entity and destination N layer entity addresses are appended to the message. This is then passed to the (N-1) layer. At this layer, the corresponding source/destination addresses for the (N-1) entities are also appended. Upon reception, the address information is stripped away as the message is passed up through the layers to its destination. The addressing is thus structured so that each layer only requires the part of the address which allows that layer to pass the message to the appropriate SAP. In Fig. 5, we show the message format adopted for WELNET as it passes from the Network layer, LLC and the MAC sublayers.

1.5 Classification of Threats in a Network

We now define a few of the terms which will be used throughout this study: A LAN is classified as an open broadcast network in which we assume messages may be received by both the intended recipient and unauthorized listeners. This will, in general, be the case unless the entire network, including the transmission media and all access points, are made physically secure. In most cases this is impractical.

The points where attacks can be made in the network are shown in Fig. 6. Here the network consists of the transmission medium, a network interface (transceiver) and the user equipment (terminal, host, etc.).

1.5.1 Low Level Threats

The types of threats present in a LAN environment can be broken down into a number of categories. The simplest form of attack is that of the passive listener (eavesdropper). In Fig. 6, we show the points in the network where the wiretapper may position the listening (recording) device. The position of the tap determines the complexity of the device, the amount of information available and the security procedures the wiretapper must overcome to gain the information. If a

tap is placed on the transmission medium, the listener can intercept messages intended for any user on the network since messages contain source/destination addressing plus virtual circuit and sequencing information (the job is much easier than that of intercepting telephone information since all signals and information required to separate them are carried on one transmission medium). If the tap is placed at the terminal connection, only information for a specific user is available, but, the wiretap device can be relatively simple and this method has the added advantage of defeating any security procedures installed in the network itself. The problem also changes with the type of LAN involved. Consider a LAN which uses a broadcast bus structure, this system has the property that it is very easy for a passive wiretapper to obtain information from the bus without detection, but it is very difficult for an active wiretapper to impersonate another transceiver without detection (assuming the operating system of the transceivers will check to determine if the header address is correct). This property is not true in a ring network where one can easily conceive of using two transceivers to surround a legitimate transceiver and originate, alter or delete messages (although how one taps into the loop without detection is not clear).

The transmission medium also plays a role in the difficulty facing an attacker. Coaxial cable is easy to tap and this can be done without interruption of service. Passive listening can be performed with a direct connection or by inductive means. An answer to this problem is the use of fibre optics but fibre optics do not lend themselves to bus architectures.

In consideration of fibre optics as the transmission medium, one also observes that they are not prone to wiretap by inductive pickup or electromagnetic emission. To tap the fibre, some portion of the signal must be diverted which, by current techniques results in detectable attenuation factors at the receiving end. To counter this problem, the attacker could introduce an active tap which would repeat the signal compensating for any attenuation, but this again necessitates interruption of the fibre which should be detectable.

1.5.2 Higher Level Threats

In the previous discussion it was assumed that the attacker was tapping the network itself to gain the information or send the messages he required. These are basically attacks against the lower layers of the OSI model. We now look at the case where the attacker has gained entry (either an authorized user making unauthorized use or someone obtaining authorized use by breaking the login procedure). From this point on the network serves merely as a transport method for accessing the service under attack. (This is shown in Fig. 7-8). All safeguards incorporated into the lower protocol levels will be nullified once valid entry is obtained.

The threats to the higher levels of the network can be quite varied. The main objective is to protect user data, data bases, hardware and the host operating system from deletion, modification, disclosure and unauthorized use. Each type of data is different and will require a differ approach to secrecy and privacy.

In this study, we will only be concerned with the problems of security in a network environment. At present, there is a strong interaction between the various LAN configurations outlined above and each will have its own repercussions when the implementation of secrecy and privacy is considered.

In the OSI model, security is introduced into level six of the model. If we look at the system model, there is a division of tasks between the network and the host computer. This division is shown in Fig. 8. Below this division, protocols are needed to protect the messages

on the network form the passive of active eavesdropper. Above the division, the network is used purely as a means of access and any attacks are directed at the host computer (we also consider here, the concept of the layered protocol is to make the operations of the underlying network transparent to the user). The isolation present in the OSI model also decouples any "real-time" protection form the upper layers, i.e., since the upper layers are independent of the lower layers such as the media access protocol, an authentication and data integrity system based on a time stamp approach could not be implemented at a high layer in the model. An example of this would be the wide variance of access times present in a moderately to heavily loaded CSMA/CD system. These examples tend to indicate that certain forms of protection must be implemented very close to the physical layer of the protocol; in addition, some of the services may be built on top of these services at the low layers, thus we can conceive of a secrecy and privacy implementation which is, itself a layered protocol which uses the services of the layers underneath it.

1.6 Network Security

The main objectives of network Security as defined in [8]-[10] are to:

i)prevent unauthorized release (disclosure) of information
ii)prevent unauthorized message addition, deletion or modification
iii)prevent unauthorized denial of resource use.

Network security can be broken down into two subtopics; 1)Secrecy and Privacy techniques and 2)Authentication and Data Integrity techniques. Secrecy and Privacy techniques are intended to provide protection against passive attacks (as per requirement (i)). Authentication deals with the ability to uniquely (and correctly) identify the originator of a message while Integrity deals with the uncorrupted transport of user messages (requirements (ii) and (iii)) in the presence of active attacks.

Many of the current approaches to secrecy and privacy are ad hoc in nature, many of them evolving as remedies for problems found in existing systems. A review of the various techniques which have been applied to networks can be found in references [11]-[15].

Part II - Observations and Implementations

2.1 Cryptanalytic Effort

The primary objectives of a secrecy system can be summarized as follows:

i)provide as much protection to the user's messages as possible (i.e. maximize the amount of work an attacker must perform in order to recover message contents)
ii) minimize the amount of information which the attacker can gain if cryptanalysis is successful (i.e. this can be done by changing keys regularly or by using multiple keys in the system)
iii) minimize the effort required to perform network maintenance i.e. to change keys, manage keys and to initiate secure communications, etc.

Observation I

It is generally accepted that, from a secrecy and privacy point of view, the use of multiple keys in a network increases the protection for users' messages and decreases the amount of information an attacker can obtain by successful cryptanalysis. Thus, it is advantageous to maximize

the number of keys in the system (ideally, each user would have its own key). Unfortunately, this leads us to deal with the problem of key management and distribution. If the number of keys is large, the problem of maintaining the security of the keys and distributing new keys requires serious consideration (this problem has been the object of considerable study [16]-[17]).

Observation II

Let's consider the effort required by the attacker to recover a key by cryptanalysis under the following assumptions:

i) a message on the network will belong to a class i , 1 <= i <= n, if it is enciphered with key K_i

ii) messages are indistinguishable before cryptanalysis (i.e. source/destination information is also enciphered as part of the message)

iii) the attacker must recover at least two messages of the same class for successful cryptanalysis

iv) the probability of a particular message being of class i is 1/n (i.e. messages of the various classes are equally likely)

v) the effort to cryptanalyze one pair of messages is 1 work unit

Under these assumptions, we can calculate the expected number of tries and thus the expected effort the attacker must make before recovering two messages of the same class. It is easily shown that the expected effort is:

$$E(W) = \sum_{i=2}^{n} i \, ((n-1)/n)^{i-2}(1/n)$$

$$= n$$

Thus, the effort required by the attacker is linear in n, that is, increasing the number of keys by a factor m simply increases the effort required by the attacker by approximately the same amount. If we now consider the effort required to manage and distribute keys and it also increases at least linearly in n (i.e. it takes twice as much effort to manage two keys as one, etc.) then nothing is gained by using multiple keys, that is, under these constraints, it is better use one key and change it regularly.

An improvement could be made if we increased the effective number of keys without increasing the actual number of keys. In the next section we will examine one method by which this could be done.

2.2 Horizontal/Vertical Keying

In part I of this paper we described the protocols of the IEEE 802 standard and the OSI model. In that section we note that the message structure was such that the address and control information for a particular level (N) is encapsulated in the frame structure of the layer below (N-1). If we expand this structure as shown in Fig. 9, we see that, even though there are n entities at the top level, the address space is the product of the address spaces at each level (i.e. two messages can share the same address at layer N but are different at the (N-1) layer. Thus a unique path through the tree is defined even if addresses at the upper layers are reused.

At this point we will introduce two terms; horizontal-keying refers to the process of assigning individual keys to each of the n entities at the uppermost layer. If we take advantage of the reuse of address space and define a set of keys the number of which is equal to the address space of that layer and use multiple encryption i.e., the message is first

encrypted with the key of the peer destination entity[2], then passed to the next lower layer where it is encapsulated and encrypted using the key of the peer destination entity of that layer (Note: by default, each half of a transaction is separately encrypted thus presenting an even more difficult task for the attacker). Assuming a block type encryption method that does not expand the message (for example DES [18]) and the multiple encryption process cannot easily be factored, then the effective number of keys is the product of the number of keys at each level while the actual number of keys is the sum of the number of keys at each level. If we look at the implementation shown in Fig. 5, where there are two layers (LLC and MAC), the maximum number of entities is:

$$n = 2^{16} * 2^{6} = 2^{22}$$

while the number of keys required in the system is

$$k = 2^{16} + 2^{6} = O(2^{16})$$

if all of the address space is used for just these two layers.

As we noted in our discussion of the addressing format, when messages (Protocol Data Units) are passed from layer N to layer (N+1), the N layer only needs to know the address of the appropriate Service Access Point (SAP) for that layer (i.e., upon delivery, address and control information is "peeled" away from the message). Thus, to implement the structured enciphering method, we must ensure that the address information is easily recoverable at each level. This could be done by i)enciphering only the message portion of the PDU leaving the address information to be enciphered at the next lower layer or, ii)enciphering the entire PDU including the addresses before passing it to the next lower layer. Upon delivery, method (i) allows the N layer to directly determine which N-SAP to pass the message to while method (ii) requires a test of all the keys at that layer (which will add overhead to the system). The advantage of method (ii) is that, even if an N-layer key is recovered, it does not reveal the grouping of messages for the (N+1) layer (i.e. which of the (N+1) layer keys the message is enciphered under).

2.3 Secrecy, Privacy, Authentication and Data Integrity

In the previous part, we noted that the IEEE 802.2 LLC standard supports two types of services; loosely coupled unacknowledged connectionless service and a tightly coupled (by sequencing, flow control and error detection procedures) connection-oriented service. The requirements for secrecy and privacy in our definitions are met by the first type of service, that is, the multiple encryption scheme prevents the attacker from easily recovering information by passive techniques. If authentication and data integrity is required, a connection oriented service should be used. The sequencing and error detection techniques integral in the service will prevent most active attacks.

Summary

We have shown that by using the hierarchical protocol structure proposed for local area networks, we can improve the difficulty presented to the passive attacker by using multiple encryption techniques. In most networks, a trade-off exists between the number of keys (which should be maximized) and the difficulty of distributing and managing the keys. By

[2] We assume here that the keys for a particular layer are known by all entities of that layer. In addition, since destination keying is performed, there is a different key used for each direction of a conversation thus providing additional difficulty for the attacker.

using the address structure used in the protocol models, we can reduce the actual number of keys by a significant factor while still presenting a high level of difficulty to the attacker.

The use of the two types of services supplied by the IEEE 802.2 standard, we can choose between a service which supports private and secret communication or one which tightly couples the communication in such a way as to allow authentication (i.e. prevention of active attacks on the network).

We also note that these features are transparent to the network users and further services can be built upon these services (e.g. a Public Key System for extra secrecy or digital signature, etc.). This area will continue to be an area of interest as more manufacturers begin to supply equipment conforming to the new standards.

Bibliography

1. D. Clark, K.T. Pogran, D.P. Reed, 'An introduction to local area networks', Proc. of IEEE, Vol. 66, No.11, Nov. 1978.
2. H. Zimmermann, 'OSI reference model - The ISO model of architecture for Open Systems Interconnection', IEEE Trans. on Comm., Vol. COM-28, Apr. 1980, pp. 425-432.
3. IEEE Project 802.1 Local Area Network Standard - Technical Report
4. IEEE Project 802 Local Area Network Standard, P802.2 Logical Link Control, Draft E, Sept 1983.
5. IEEE Project 802 Local Area Network Standard, P802.4, Draft IEEE Standard 802.4, Token Bus, Draft D, Dec. 1982.
6. IEEE Project 802 Local Area Network Standard, P802.5, Draft IEEE Standard 802.5, Token Ring, Dec. 1983.
7. J. Mark, J. Field, J. Wong, T. Todd, J. McMullan, G. Agnew, 'WELNET A High Performance Local Area Communications Network', CCNG report series, Dept. of Elec. Eng., Univ. of Waterloo, May 1983.
8. W. Diffie, M. Hellman, 'Privacy and authentication : An introduction to cryptography', Proc. of the IEEE, Vol. 67, March 1979, pp. 397-427.
9. S.T. Kent, 'Security requirements and protocols for a broadcast scenario', IEEE Trans. on Comm., Vol. COM-29, June 1981, pp. 778-786.
10. V. Voydock, S. Kent, 'Security Mechanisms in High-Level Network Protocols', Computing Surveys, Vol 15, June 1983.
11. D. Parker, 'Computer abuse perpetrators and vulnerabilities of computer systems', NCC'76, June 1976, New York, pp. 65-73.
12. N. Nielson, B. Ruder, D. Brandin, 'Effective safeguards for computer system integrity', NCC'76, June 1976, New York, pp. 75-84.
13. E. Gudes, H. Koch, 'The application of cryptography for data base security', NCC'76, June 1976, New York, pp. 97-107.
14. G. Purdy, 'A high security log-in procedure', Comm. of ACM, Vol. 17, Aug. 1974, pp. 442-445.
15. B. Walker, I. Blake, 'Computer Security and Protection Structures' Dowden,Hutchinson, Ross, Stroudsburg, Penn., 1977.
16. I. Ingemarsson, D.T. Tang, C.K. Wong, 'A conference key distribution system', IEEE Trans. on Info. Theory, Vol. IT-28, Sept. 1982, pp. 714-720.
17. W. Chou, A. Nilsson, 'Key distribution and authentication procedures in internetworking environment', Computer Networking Symposium, National Bureau of Standards, Maryland, Dec 1982, pp. 50-54.
18. 'Data Encryption Standard', National Bureau of Standards, Federal Information Processing Standard (FIPS), Pub. No. 46, Jan. 1977.

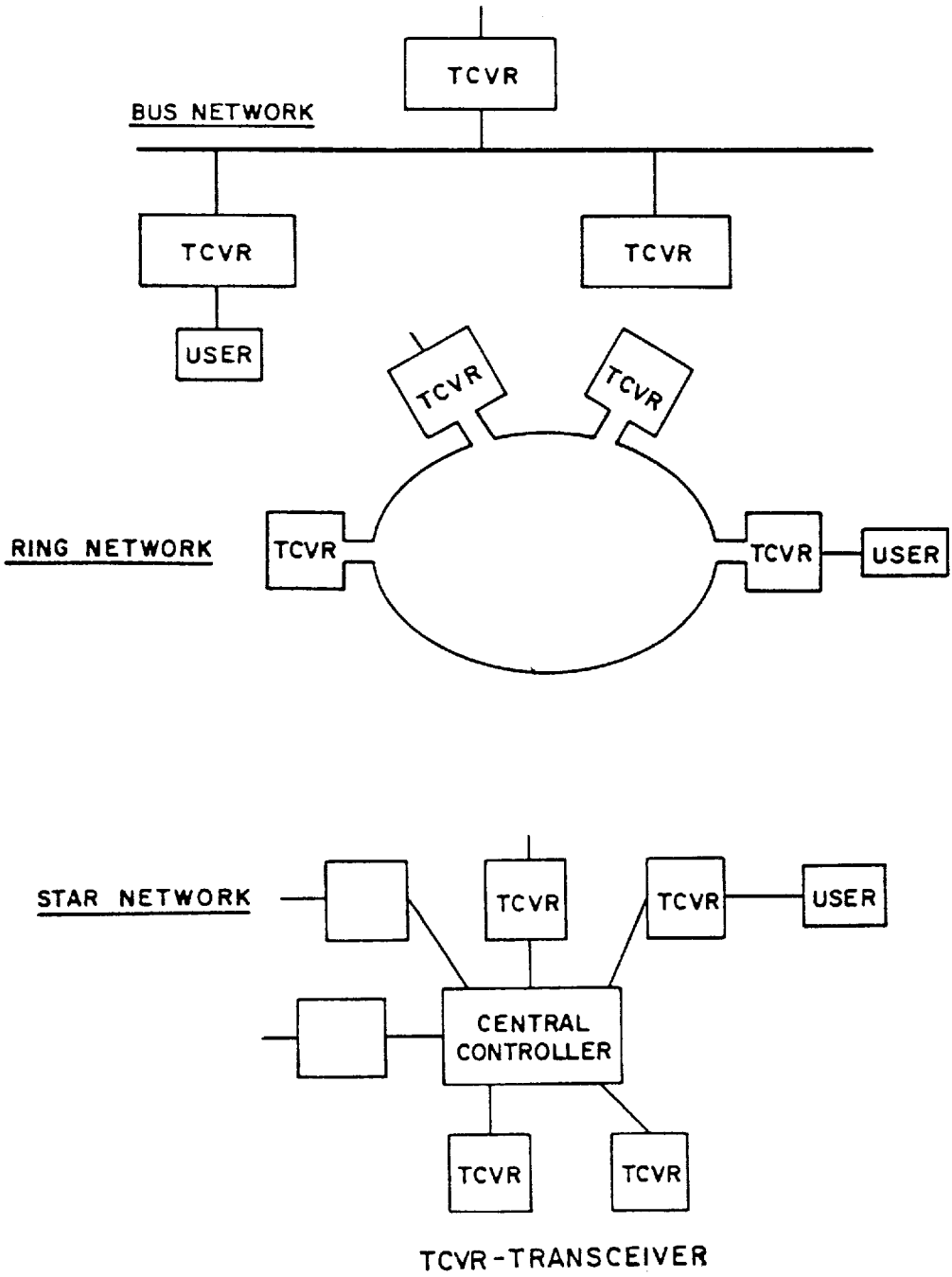

Fig. 1 Typical LAN Configurations

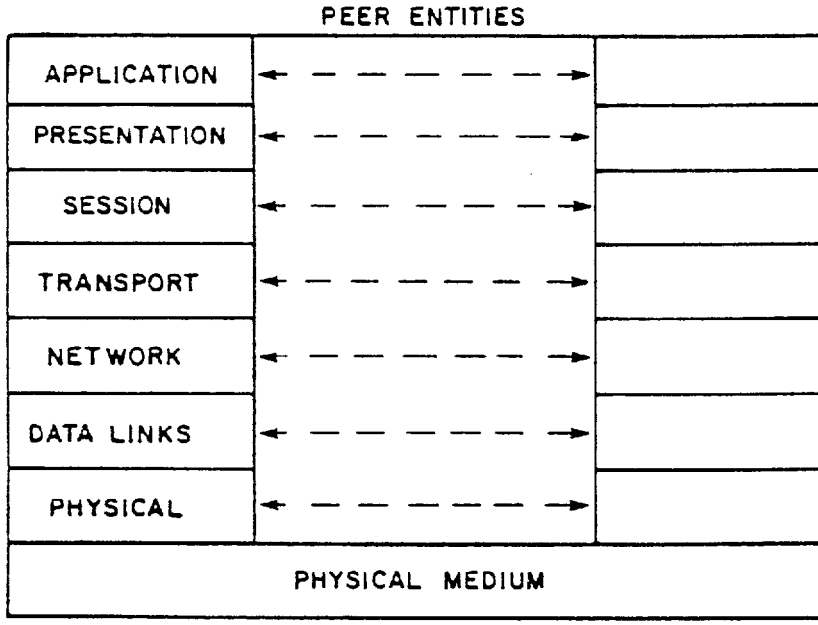

Fig. 2 Open Systems Interconnection Model

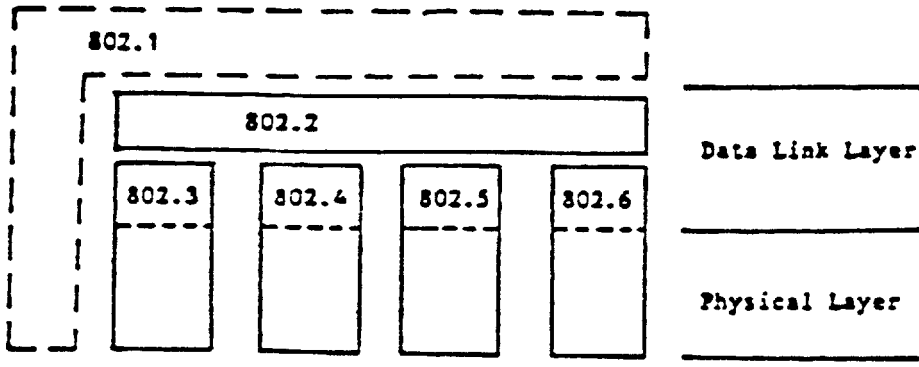

Fig. 3 IEEE Project 802 Format

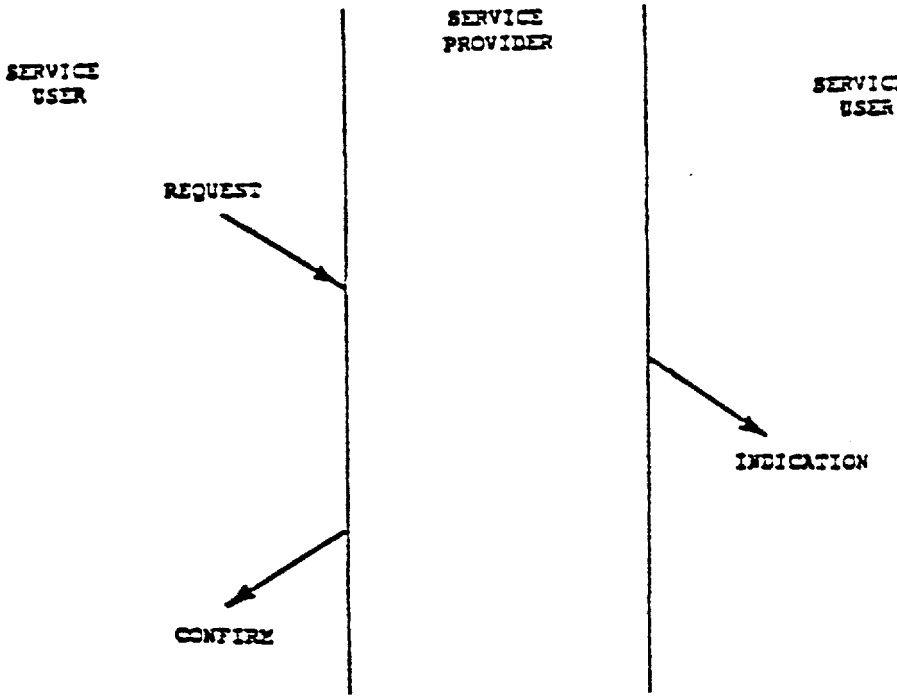

Fig. 4 Format for Service Primitives

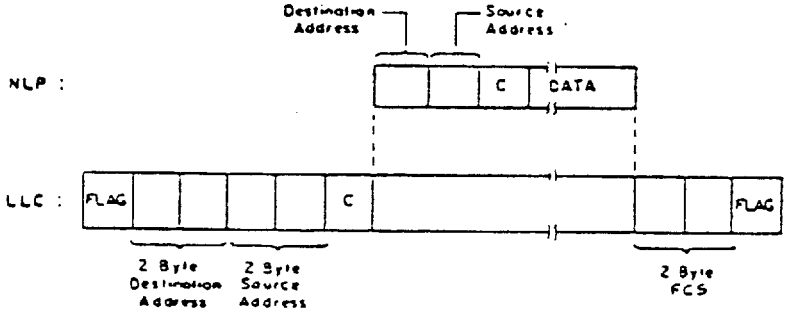

Fig. 5 Address and Data Format for Network Layer and LLC

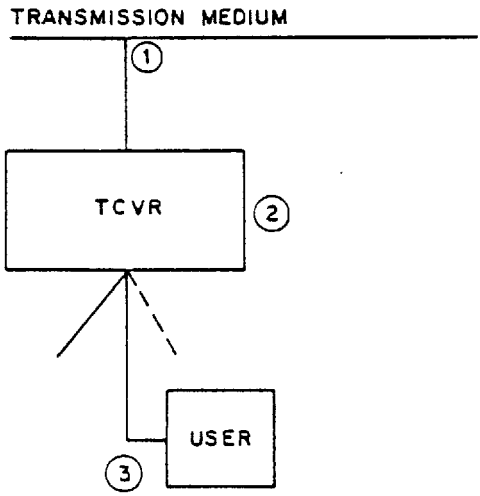

Fig. 6 Points of Attack in a LAN

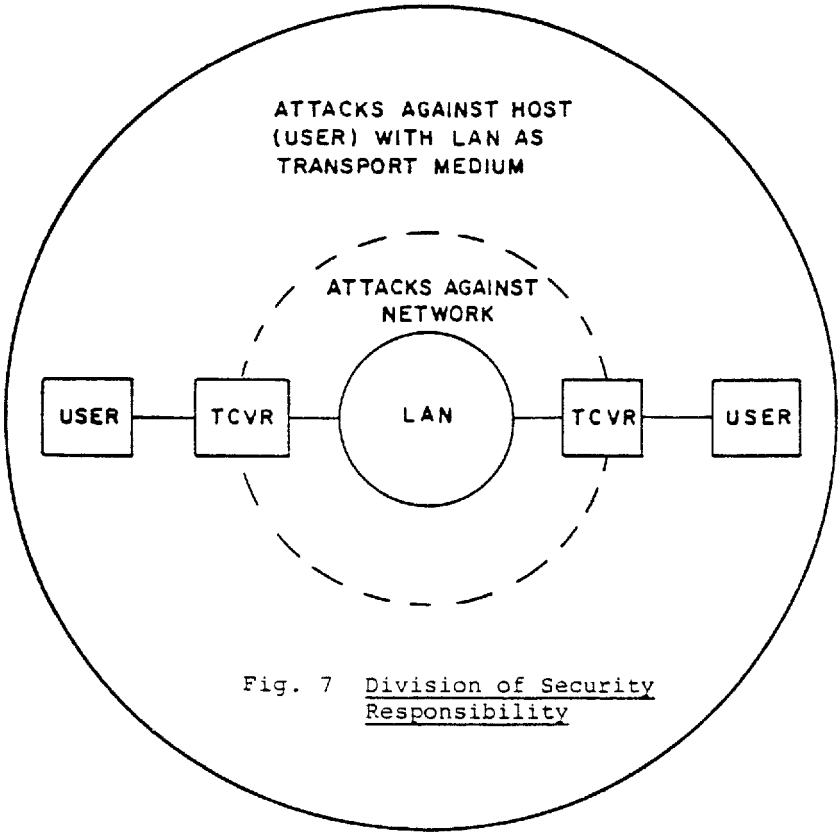

Fig. 7 Division of Security Responsibility

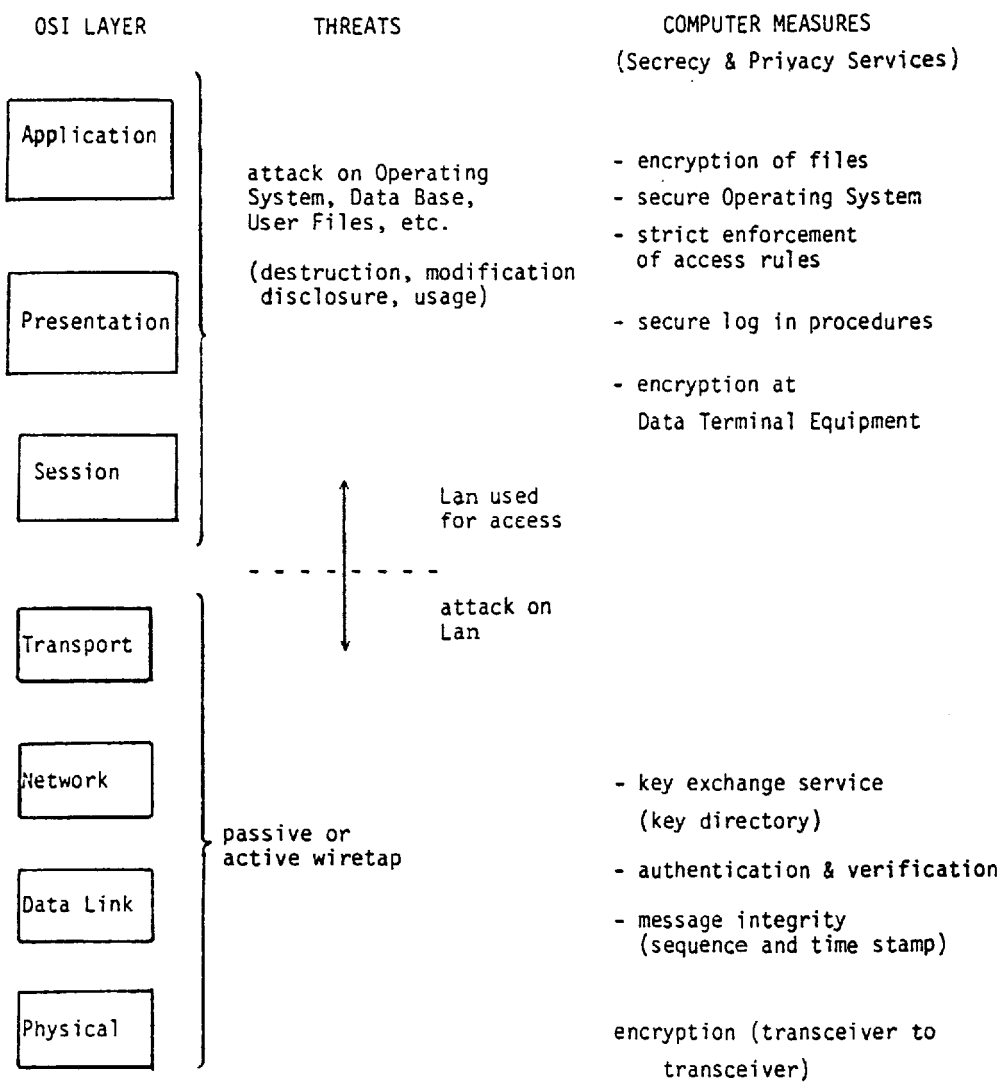

Fig. 8 Network Structuring for Secrecy and Privacy

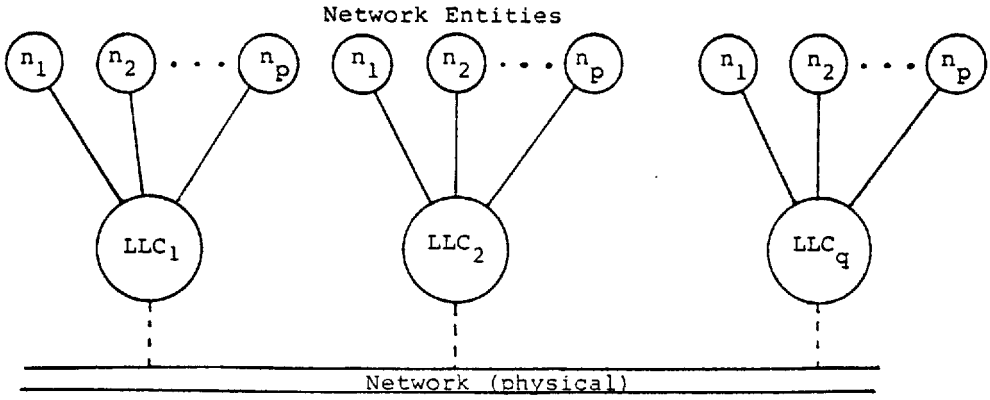

Fig. 9 Structuring of Network Entities and Addresses