MODELING OF ENCRYPTION TECHNIQUES FOR SECRECY AND PRIVACY IN MULTI-USER NETWORKS

G.B. Agnew
Computer Communications Networks Group
University of Waterloo
Waterloo, Ontario, Canada
N2L 3G1

Much of the present literature on computer security deals with cryptographic methods and cryptanalytic attacks. Most of these systems are based on dedicated communication links or single computer systems. In this study, we examine some aspects of incorporating cryptographic methods into multi-user systems by exploiting the underlying network structure.

A multi-user network provides the physical and procedural facilities to establish and operate a communication path between any two or more users. Here, we define a user as the smallest uniquely identifiable entity in the network (later we will distinguish between users and groups of users which are multiplexed into a larger entity). We also define an association as a communication path established between any subgroup of the set of users. (To simplify our analysis, we will only consider associations between two users, one designated the source (S), and the other the destination (D).)

A broadcast channel is a common communication channel where messages are 'heard' by all users. To use the broadcast channel yet preserve the separation of messages into their respective associations, some form of addressing must be performed. In networks in which the associations are not determined apriori (e.g., Time Division Multiplexing), messages will usually consist of two parts; the data portion of the message and the header portion which uniquely defines the association (see Fig. 1).

The nature of broadcast channel also aids the attacker in his job. In a purely passive attack (passive wiretap), the attacker has access to all of the channel messages. The presence of header information

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 221-230, 1986.

allows him to selectively intercept messages. Even if the data portion of the message is obscured, the existence of an association may provide sufficient information to the attacker (traffic analysis). In active attacks (active wiretap), the attacker may try to systematically insert, delete or modify messages.

If the physical portion of the network cannot be protected from active or passive attacks, then cryptographic techniques (encryption) must be used to thwart the attacker. Encryption methods are divided into two classes, i) one-key (symmetric) encryption techniques where the encryption and decryption functions are closely related and one cannot be exposed without compromising the other, and, ii) two-key (public key) encryption techniques where separate encryption, decryption functions are used. At present (and in the foreseeable future), two-key systems are very restricted in throughput. Hybrid systems are generally used where two-key methods are used to exchange the keys which are used in higher throughput one-key systems. In our approach, we will assume that such a mechanism exists to exchange keys which will be used to encipher data for transmission on the high bandwidth channel. The actual encryption may be of two forms; stream encryption where message bits are combined with a stream of enciphering bits and, block encryption where messages are divided into blocks (generally fixed size) which are then enciphered as a unit. We will not distinguish any further between these methods, but our examples will only consider fixed block size encryption methods such as the National Bureau of Standards Data Encryption Standard (DES) algorithm which operates on 64 bit blocks with a 56 bit key.

In the network environment, we consider two levels of protection that encryption can provide: i) Secrecy where messages from one association are completely isolated from external observers and all other network users (this requires a secret encryption function unique to each association) and, a less stringent form of protection, ii) Privacy where messages are only protected from external observers (i.e., a common encryption function could be used by all associations).

Systems using Multiple Encryption Functions

In the absence of apriori information such as known ciphertext or chosen plaintext, the passive wiretapper is forced to use cryptanalytic methods to recover the content of messages. In block encryption methods, the cryptanalytic strength lies in the difficulty of removing the uncertainty of the enciphering key H(K). This usually involves the accumulation of sufficient quantities of text enciphered under one key to recover that key [3], [5].

We now examine some properties of systems which have one or more enciphering keys.

Let $\underline{K}$ be the ensemble of network keys $\underline{K} = \{K_1, K_2, \ldots, K_N\}$. The uncertainty associated with this ensemble is [5],

$$H(\underline{K}) = H(K_1, K_2, \ldots, K_N)$$
$$= H(K_1) + H(K_2|K_1) + H(K_3|K_1, K_2) + \ldots .$$

if all of the keys are independent and identically distributed (iid) and H(K) is the average uncertainty of a key, then

$$H(\underline{K}) = N * H(K)$$

We note in passing that this does not suggest that the key ensemble could be replaced by an equivalent key of size N * k, where k is the size of one key. This would result in a privacy only system. We can see this in another way if we examine the effect of successfully cryptanalysis on part of the ensemble. Let $\hat{}H(\underline{K})$ be the normalized change in system uncertainty when a key K_i is recovered. In an N key ensemble

$$\hat{}H(\underline{K}) = \frac{N * H(K) - (N-1) * H(K)}{N * H(K)}$$
$$= \frac{1}{N}$$

This shows that the impact to the network caused by disclosure of cryptanalytic recovery of a key can be reduced by increasing the number of keys. Ideally, each association would have a unique key. This of course introduces other problems as discussed in [4].

Despite our ability to increase the ensemble uncertainty $H(\underline{K})$, we are still constrained to an individual key uncertainty of H(K). In the next section, we consider ways of increasing the apparent or observed key uncertainty H(K'), that is, the key uncertainty as observed by the passive wiretapper.

The passive wiretapper's observation of the communication channel is modeled as shown in Fig. 3. Here a random plaintext message M is selected from the set of all messages of length m. This message is then enciphered by all functions $Y_i = E_i(M)$ where enciphering function i is determined by key K_i which is selected at random for each box from the set of all keys of length k. The channel output Y_i is then selected at random from the N enciphering functions as indicated by the output switch position. This operation simulates the random message arrival process in a multi-user network.

In terms of the channel observation, we define a message to be of class c, $c \varepsilon C = \{1, 2, \ldots, N\}$, if it is enciphered under key K_c. By our model, the apparent key uncertainty is equal to the joint uncertainty of the key K and the message class C.

$$H(K') = H(K,C)$$
$$= H(K|C) + H(C)$$

If the keys are chosen independently of the class of the message, then

$$H(K') = H(K) + H(C)$$

If the attacker knows the switch position, then $H(C) = 0$ and there is no gain over the individual key uncertainty. On the other hand, if the switch position can be hidden and is equally likely among the N classes then,

$$H(C) = \log_2 N \text{ bits}$$

and

$$H(K') = K(K) = \log_2 N \text{ bits}$$

This is shown in Fig. 4 for a system with $H(K) = 56$ bits.

Thus, we can increase the observed uncertainty of an individual key by (at most) $\log_2 N$ bits by obscuring the message class information.

Let us now consider the case where messages can be enciphered by the source user in such a way that they can be uniquely identified and recovered by the destination user (this is code division multiple access (CDMA)). As we have mentioned previously, an association is identified by its source and destination. If we associate a separate enciphering function with each association, then the uncertainty of the message class is the joint uncertainty of the source S and destination D.

$$H(C) = H(S,D)$$
$$= H(S) + H(D|S)$$

If the selection of source and destination is independent and identically distributed among U users, then

$$H(C) = H(S) + H(D)$$
$$= 2\log_2 U$$

(In reality, there would only be $U * (U-1)$ possible associations, but we will approximate this by U^2.)

This indicates we can hope to gain $2\log_2 U$ bits of uncertainty, but, as we shall see, will not be possible.

Effects of Network Scheduling

There are two broad classes of network access methods: i) random access techniques and ii) conflict free (fully scheduled) techniques. In random access techniques (such as CSMA and CSMA/CD), a user wishing to transmit a message waits until the channel is silent, then begins transmitting. This technique leads to loss of transmission bandwidth due to message collisions when two or more users try to transmit at the same time. To make better use of the bandwidth available on the channel, scheduling techniques such as token passing are used to elimin-

ate contention among the users [6].

These differences also have an effect on the level of system security. This can be seen in the following way: if the attacker can observe the scheduling mechanism (this could be done by observing the token passing or simply counting modulo the number of users in the system), then the attacker can observe the message source thus removing $\log_2 U$ bits of uncertainty (i.e., there will always be the equivalent of $\log_2 U$ bits of information in the scheduling scheme if the system is capable of resolving all contention among U users). Recall that

$$H(C) = H(S) + H(D|S) \leq 2\log_2 U \text{ bits}$$

If the scheduling information is available to the attacker, then $H(S) = 0$, that is scheduling information is equivalent to knowing the message source. We now have the condition that

$$H(C) = H(D|S)$$

which can only reach $\log_2 U$ bits if the destination is independent of the source. This indicates that the deterministic properties of the scheduling which are used to improve the performance of the network, also help the attacker gain information.

In random access systems, the lack of scheduling information should improve the gain in observed key uncertainty, that is, we should be able to gain $H(C) = \log_2 U$ bits. In an ideal network, this would be possible, unfortunately, it can be shown that, if we allow analog attacks on the network, the source information can still be recovered (see [7]).

In the above discussion, we have shown that a gain in the apparent key uncertainty can be realized if the destination user is independent of the source. We shall examine this condition with respect to the network protocol structure. In the International Standards Organization's (ISO) model for Open Systems Interconnection (OSI), seven layers of protocol for networks have been defined [8]. The uppermost layers contain protocols which deal with individual users. At the lowest level (Physical layer), we deal with network transceivers (TCVRs) as an identifiable entity.

The protocols are structured such that several layers of multiplexing can exist between the user levels and the physical level. Thus many users may be associated with one TCVR. The throughput requirements and nature of messages of the two levels may also be quite different. Consider the case where we have a number of terminals connected to one TCVR. In most cases, the individual terminal throughput requirements will be relatively small. In addition, associations at the terminal level tend to exist for comparatively long periods (this will permit us to set up protocols to generate and exchange keys on a per association basis). At

the physical level, the throughput requirements are much higher due to the concentration effect of the terminal traffic. We also note, that consecutive TCVR messages may have different destination (e.g., terminals may be associated with hosts connected to different TCVRs). Thus, multplexing above the physical layer may produce the desirable effect (cryptographically), of making the destination TCVR independent (from message to message) of the source.

The network structure also divides the protection which can be provided at each layer. For user secrecy, encryption must be applied where the user is an identifiable entity, that is, at the upper protocol layers (end-to-end encryption). Encryption at the physical layer can be used to provide privacy and prevent traffic analysis.

If encryption is performed at the upper layers on a per association basis, then the data portion of the messages passed to the physical layer will already be enciphered. This implies that the physical level encryption is required to protect only $\log_2 U$ bits of information. For example, if the system has U = 256 users, the physical layer requires a minimum of 8 bits of class uncertainty. In practice, this could be provided by a single key using the Data Encryption Standard.

In the next section, we look at some of the benefits and problems of implementing a CDMA system at the physical level.

Implementation of Code Division Multiple Access

As discussed previously, in a multi-user, random access system, we must dedicate some portion of the message to address information. This requires at least $\lceil \log_2 N \rceil$ bits of header information to uniquely identify a destination in an N transceiver system. If the messages are M bits in length, there are 2^M possible messages. We define a message as being a valid or meaningful message for a particular transceiver if the first $j = \lceil \log_2 N \rceil$ bits match a bit pattern unique to that transceiver (address). Thus there are 2^{M-j} valid messages for each transceiver (the message space is partitioned into 2^j non-overlapping sets of messages). We observe that any M bit string will be a valid message for at most one transceiver (in the absence of channel errors). We define address aliasing as the condition where a message is valid message for two or more transceivers (i.e., the message space partitions are overlapping).

In a system with headers as described above, an attacker can always generate a message which appears valid to a particular user simply by attaching that users address to the beginning of an (m-j) bit string. We shall call this type of attack a spoofing attack on a selected transceiver. If $j > \lceil \log_2 N \rceil$, then some strings will not be valid messages

for any transceiver.

We define the spoofing probability P_{sp} as the probability of a random message being valid for at least one transceiver. In this case

$$P_{sp} = N/2^j$$

To provide protection from traffic analysis and spoofing attacks, the system can incorporate header encryption as discussed previously. To preserve the ability to address individual transceivers, we must again allocate some portion of the message to identification (at least $\lceil \log_2 N \rceil$ bits). There are two basic methods by which we can achieve this addressing, i) we could use one transform common to all transceiver and use the transceiver's address in the header, or, ii) we could define a unique transform for each transceiver and require the deciphered message to match a bit pattern in the header. In the first system, the enciphering transform defines a specific one-to-one mapping of the ciphertext space into the message space. Thus, if the message space is divided into non-overlapping partitions, then the ciphertext space will be similarly partitioned.

Without knowledge of the encryption transform, the attacker can do no better than try a random message to spoof the system so,

$$P_{sp} = N/2^j$$

as for the unenciphered case. In the second case though, the use of multiple enciphering functions produces a different effect. The probability of a random message being valid for one transceiver is 2^{-j}. If we assume that our enciphering functions are independent, then the probability of spoofing is equal to

$$\begin{aligned} P_{sp} &= 1 - \Pr(\text{a random message is not a valid message for any of the N transceivers}) \\ &= 1 - (1 - 1/2^j)^N \end{aligned}$$

Which is strictly less than $N/2^j$ for $N > 1$. Thus, using multiple enciphering functions can improve the resistance of the system to random spoofing attacks. But, multiple enciphering functions have other effects. If we now consider the probability of address aliasing, we can define

$$\begin{aligned} &\Pr(\text{address aliasing}) \\ &= \Pr(\text{message is valid for at least one other TCVR} \mid \text{it is a valid message for one}) \\ &= 1 - (1 - 1/2^j)^{N-1} \end{aligned}$$

that is, it is directly related to the spoofing probability. This implies that if we try to isolate data passed at the physical layer by using multiple enciphering functions, we can improve the immunity to spoofing attacks but we also increase the probability of address aliasing occurring. (Even though we cannot provide user isolation at the physical

level, we might use multiple enciphering functions to separate groups of users on the same network.)

The above result indicates that to reduce the probability of aliasing and simultaneously reduce the probability of an attacker generating false messages, we should ensure that the header sequence is large with respect to the number of users, i.e., $j > \log_2 N$ bits.

Remarks

The incorporation of cryptographic techniques into a multi-user network is a very complex problem. In this study, we have analysed a few of these problems and have provided some guidelines for implementation. We show that, both from a user isolation (secrecy) and system protection point of view, maximizing the number of system enciphering functions is desirable. If we are constrained to a fixed size for individual encryption keys, we can increase the apparent key uncertainty as observed by the attacker by an amount equal to the uncertainty of a message's destination. We have also shown that the way in which we implement a code division multiple access scheme will affect the ability of the attacker to generate false messages and the probability of the system itself to generate meaningful messages for more than one transceiver.

Bibliography

1. V. Voydock, S. Kent, 'Security Mechanisms in High-Level Network Protocols', Computing Surveys, Vol. 15, pp. 135-171, June 1983.

2. National Bureau of Standards, 'Data Encryption Standard', FIPS PUB 46, Washington, D.C., Jan. 1977.

3. M.E. Hellman, 'A Cryptanalytic Time-Memory Tradeoff', IEEE Trans. on Info. Theory, IT-26, pp. 401-406, July 1980.

4. G. Agnew, 'Secrecy and Privacy in a Local Area Network Environment', Proceeding of EUROCRYPT '84, Paris, Apr. 1984.

5. C.E. Shannon, 'Communication Theory of Secrecy Systems', Bell System Technical Journal, Vol. 28, pp. 656-715, Oct. 1949.

6. J. Mark, J. Field, J. Wong, T. Todd, J. McMullan, G. Agnew, 'WELNET, A High Performance Local Area Communication Network', Computer Communications Networks Group, University of Waterloo, Report E-114, May 1983.

7. G. Agnew, 'Encryption in a Multi-user Network' Computer Communications Networks Group, Report CCNG E-124, University of Waterloo, Dec.1984.

8. H. Zimmerman, 'OSI reference model - The ISO Model of Architecture for Open Systems Interconnection, IEEE Trans. on Comm., COM-28, pp. 425-432, Apr. 1980.

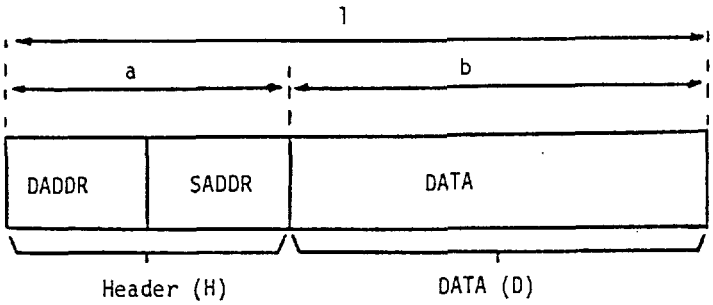

Fig. 1 Message Format

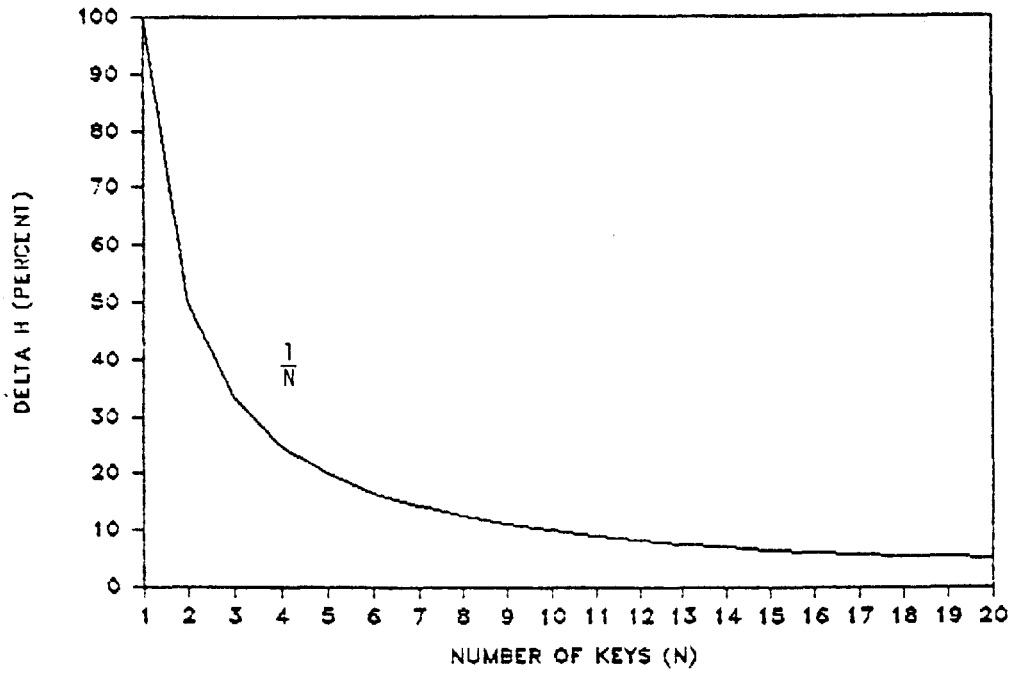

Fig. 2 Relative Change in System Uncertainty

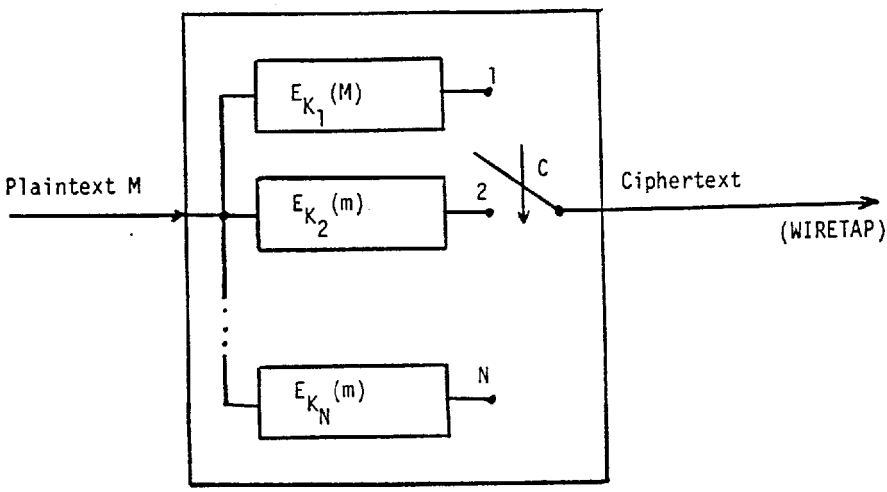

Fig. 3 Channel Model as Observed By Attacker

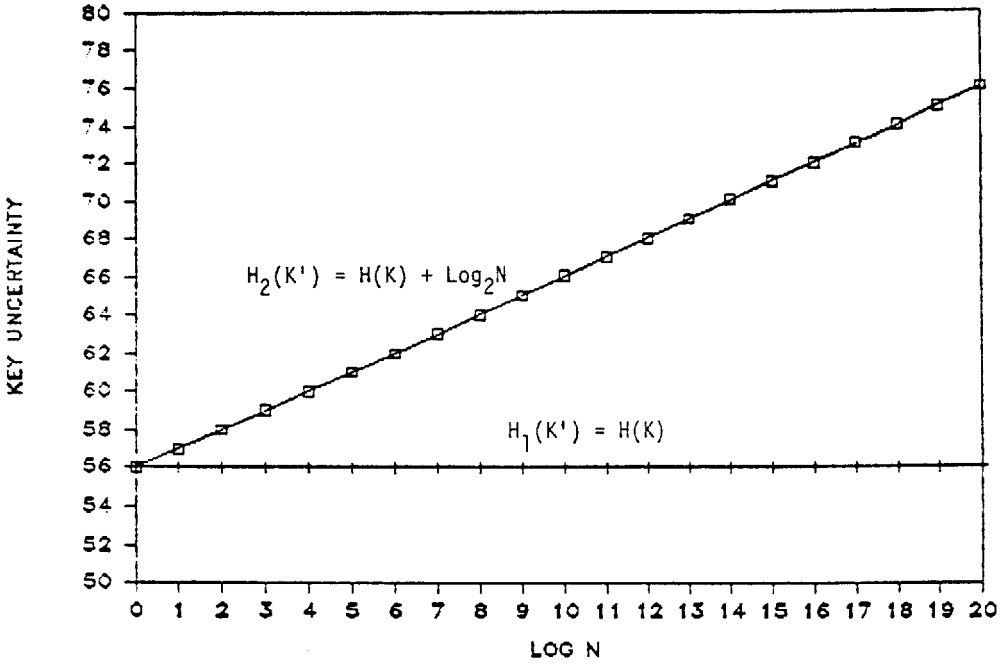

Fig. 4 Comparison of Observed Key Uncertainty with and without Header Encryption