Fault Tolerance for Link Encryption in ATM Systems

Andreas Rieke

Abstract— **The main purpose of this paper is to demonstrate different possible variants of link encryption in ATM systems. In particular, the encryption method proposed by the ATM Forum is discussed and compared to two different methods proposed in this paper. The main difference between the two methods is the fact that in one of them, not only the payload of a cell, but also the ATM header is subject of encryption.**

I. Introduction

DATA encryption is required to provide privacy in communication channels and links, as in the Asynchronous Transfer Mode (ATM). Amongst different encryption techniques, link encryption is considered in this paper.

Link encryption in this context means the encryption of data which are transmitted over a link from one switch/endpoint to another one. Only repeaters are allowed as intermediate nodes in a link.

The essential questions to be discussed in this paper are which data are subject to encryption and which mode of operation is to be used.

Link encryption is often used to encrypt only the relevant data transmitted on a link. Synchronisation data and other less sensitive data are therefore often transmitted unencrypted. In this context, the question arises whether the ATM header and operation and maintenance (OAM) cells are to be encrypted or not.

Due to different characteristics of encryption algorithms and modes of operation, the choice of a suitable function is an important task. It is not the scope of this paper to select a specific encryption algorithm, because this is not only a technical task, but also depends on the patent situation and licence fees. Instead, the different modes of operation with characteristics including cryptographic synchronisation and fault tolerance will be discussed.

The properties of these modes are analysed and referred to ATM systems in section II. Section III gives a summary of current activities concerning encryption in the ATM Forum. In section IV, a cell payload encryption system is proposed.

If only the payload of ATM cells is encrypted, the header is transparent to aggressors. It is possible to recognise how many virtual connections are in use; for each virtual connection, characteristics as the bit rate can give information on the service that is being used.

If the header is encrypted, too, listening to a link does not reveal any information: perfect anonymity of communication is achieved.

A solution for complete cell encryption is given in section V. Some concluding remarks are given in section VI.

A. Rieke is with the Forschungsinstitut für Telekommunikation (FTK), Dortmund, Germany. E-mail: andreas.rieke@fernuni-hagen.de

II. Properties of the different modes

In this context, four modes of operation are considered. In case of block ciphers, the ECB (electronic codebook) and CBC (cipher block chaining) modes of operation are chosen, whereas, in case of stream ciphers, synchronous and self-synchronising stream ciphers are concerned.

These four basic modes of operation differ significantly in properties like cryptographic synchronisation and fault tolerance. These properties are discussed in the following section and are referred to link encryption in ATM systems.

A. Cryptographic synchronisation

Cryptographic synchronisation is guaranteed in normal operation. But in case of start of operation or disturbance, it is necessary to gain synchronisation again.

In the physical layer of ATM systems, discarding of cells may occur in the header sequence generation/verification function. As long as the number of discarded cells is known, this phenomenon is called detected cell loss and does not affect cryptographic synchronisation. Undetected cell loss is not possible in the physical layer as long as the cell delineation function works synchronised.

All modes of operation except the synchronous stream cipher are self synchronising. Therefore, cryptographic synchronisation will be reached immediately in ECB mode and one block after start of operation or undetected cell loss in the other modes. In case of the synchronous stream cipher, some kind of signalling must be performed to reach cryptographic synchronisation when the cell delineation function has gained synchronisation.

In the ATM layer, undetected cell loss may occur due to the header sequence verification or cell rate decoupling function. Therefore, cryptographic synchronisation is not guaranteed in the ATM layer.

B. Fault tolerance

In this subsection, the effects of bit errors are analysed. The encrypted data stream is affected by bit errors and the result of the decryption function is compared to the equivalent system without encryption.

The synchronous stream cipher is the only cipher that causes no error multiplication, as long as cryptographic synchronisation is given. A cipher in ECB mode with block length l causes l random bits after decryption of a faulty block. Block ciphers in CBC mode cause an error of l random bits in the affected block, but also a single bit error in the next block. Self-synchronising stream ciphers with an internal state of l bits cause a single bit error, followed by l random bits.

III. Current activities in the ATM Forum

In October 1995, a security working group was established in the ATM Forum. At the time of writing this paper, the sixth revision of a draft security specification [1] was available.

The structure of this draft is mainly divided in

- security services for the user plane,
- security services for the control plane and
- support services.

In the current revision, security services in the control plane is just authentication, whereas in the user plane, confidentiality, integrity of data and access control are additionally specified.

User plane confidentiality is defined for two scenarios: endpoint-to-endpoint and switch-to-switch. Both scenarios are not specified as link encryption, because intermediate nodes like switches are allowed even if these nodes do not support ATM security services. Therefore, the encryption is not link-oriented, but connection-oriented, that means, for each virtual connection a unique key may be used. Confidentiality is provided at the ATM layer at the ATM cell level. Because of intermediate switches, encryption or modification of the ATM cell header is not possible.

The specification includes the definition of a set of default algorithms for interoperability, but allows vendor-specific extensions. Default algorithms are DES [2] with a 56 bit effective key, Triple DES with a 112 bit effective key and FEAL [3] with a 64 bit key, no key block parity and N=32. When using one of the previous algorithms, ECB, CBC or counter mode are the recommended modes of operation. The synchronisation and error propagation characteristics of counter mode are identical to those of output feedback (OFB) mode; for this reason, resynchronisation algorithms are specified in this mode of operation. IDEA (international data encryption algorithm, [4]) is not (yet) specified for user plane data confidentiality.

IV. Cell payload encryption

In case of cell payload encryption, the header of the ATM cell is not encrypted. Since the length of the payload of ATM cells (384 bits) consists of an integer multiple of the block length of common block ciphers (64 bits), encryption can be performed on the basis of single cells in all four modes of operation.

In ATM systems, OAM information is – among other things – used to control physical links. This information is transmitted in ATM cells in cell based transmission systems. OAM cells are processed by repeaters, switches and endpoints.

Since repeaters should not have access to secret keys, these cells must be transmitted unencrypted. On the other hand, crypto signalling cells must also be transmitted unencrypted in order to recognise them even if cryptographic synchronisation is lost. Due to specific header patterns for these cells, the decision whether to encrypt or decrypt a cell makes no problem.

The cell payload is processed in the ATM adaptation layer (AAL). In this paper, the effects of bit errors in AAL 1 and AAL 5 are analysed as examples, because AAL 1 and AAL 5 are the most important AALs today.

For the analysis, it is assumed that a single bit error in the payload of an encrypted cell leads to a block of length l of random bits after decryption. Therefore, the effects of error multiplication caused by encryption are considered.

In case of AAL 1, the performance of the segmentation and reassembly (SAR) sublayer and lower layers is analysed assuming random bit errors. The performance is assessed in terms of the probability of wrong sequence number or invalid status.

Fig. 1 shows the influence of error multiplication on AAL 1 SAR and lower layers performance. It is obvious that link encryption with error multiplication significantly reduces the performance compared to the not encrypting system.

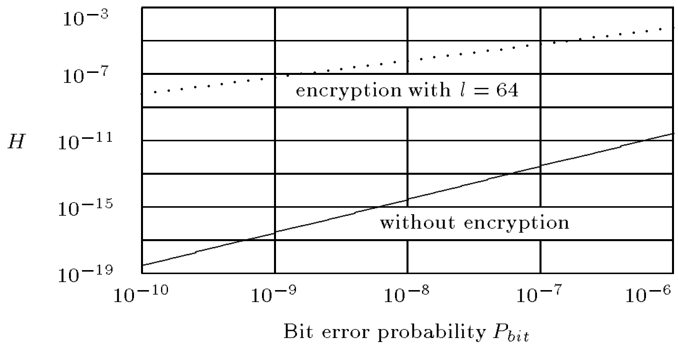

Fig. 1. Influence of error multiplication on AAL 1 SAR and lower layers performance
H: probability of wrong sequence number or invalid status

In case of AAL 5, packets of data are segmented into ATM cells and reassembled at the receiving end. A 32-bit cyclic redundancy check (CRC) is used to check the correctness of the packet [5]. Therefore, a single bit error in the not encrypting system can be detected reliably.

Since the number l of random bits is usually larger than the degree of the CRC, a single bit error in case of encryption with error multiplication leads to an error that can not reliably be detected.

Due to the advantages of the synchronous stream cipher, it is obvious that the synchronous stream cipher is best suited for cell payload encryption.

The cell payload encryption function must be implemented above the HEC header error sequence generation/verification function in order to work with the eventually corrected cell header. Since the synchronous stream cipher needs cryptographic synchronisation, it is to be implemented below the cell rate decoupling function.

V. Complete cell encryption

In ATM systems, the HEC-field (header error control) of the cell header is not only used to protect the header against transmission errors; the cell delineation function also uses this field. For this reason, it is not possible to encrypt the HEC-field; it must be calculated from the encrypted cell header. Therefore, complete cell encryption in this paper always means encryption without the HEC-field.

The main problem in the complete cell encryption function is the following: Some cells that are not encrypted (OAM cells in cell based transmission systems, crypto signalling cells) can not reliably be distinguished from encrypted cells. Thus, cells must be coded in a way that this distinction becomes possible.

The idea is to use one bit of the HEC for this purpose. This bit is called encryption bit.

The HEC-field is calculated by the header sequence generation/verification function. In correction mode, single bit errors can be corrected and double bit errors can be detected; in the latter case, the cell will be discarded. After an error occurs, the next cell is processed in detection mode. Reliable detection of at most three bit errors is possible, but correction is not carried out. If a cell seems to be without errors in detection mode, the next cell is processed in correction mode again. Header error correction is performed with a generator polynomial of degree 8 ($x^8 + x^2 + x + 1$) of a cyclic code [6, p. 17].

It was shown that this polynomial is not well suited for header error control in case of ATM cells; polynomials of degree 7 can also reach the capabilities described above, even if one additional bit is to be protected [7].

To avoid additional synchronisation problems, ECB and CBC mode are not considered, since the usual blocklength of 64 bits is not suited to encrypt cells with 416 bits length. In order to decide which of the remaining modes is more suitable for a complete cell encryption function, an analysis on effects of bit errors has been performed.

Since the synchronous cipher does not cause error multiplication, only the self-synchronising cipher is considered. It is assumed that single bits are processed without interleaving.

In case of single bit errors, it is assumed that cell i is hit. This error may lead to an erroneous internal state which might influence the decryption of the following cells. The probability that cell $i+1$ has a header error is given in fig. 2.

Again, it is obvious that error multiplication considerably reduces the performance of the system. Therefore, the synchronous stream cipher is the best choice in this case, too.

The cipher must be implemented below the cell rate decoupling function in order to guarantee synchronisation. Since the HEC is calculated from the encrypted cell header, decryption must take place after header sequence verification.

VI. Conclusions

It is not admissible to compare the ATM forum encryption scheme or other schemes like [8] directly with the proposals in this paper. These schemes are not link encryption schemes; connection oriented encryption is used over more than one link with intermediate switches even if these do not support ATM security services.

It is shown that error multiplication produced by the decryption function significantly reduces the performance

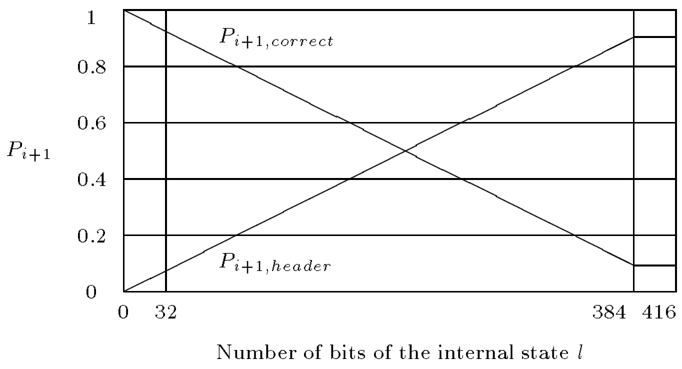

Fig. 2. Effects of a single bit error in cell i using a self-synchronising stream cipher

of the system. All known self-synchronising ciphers cause error multiplication. Due to this fact and other advantages two link encryption schemes are proposed in this paper, where the synchronous stream cipher that works without error multiplication is preferred.

With little expenditure, a cell payload encryption system can be integrated in future ATM-switches. Complete cell encryption causes higher expenditure, but results in a higher level of security.

In future, the proposed solutions can also be applied in photonic networks. A link in photonic networks can reach from one endpoint to the other; thus, end-to-end encryption is additionally provided in this case.

This work was carried out at the Institute of Communication Systems, University of Hagen, Germany under the supervision of Prof. Kaderali. I would like to thank Prof. Kaderali and my colleagues for interesting discussions.

References

[1] The ATM Forum, Technical Committee, *Phase I ATM Security Specification (Draft)*. ATM Forum BTD-Security-01.00, 1996.

[2] U. S. Department of Commerce, National Bureau of Standards, *Data Encryption Standard*. Federal Information Processing Standards Publication (FIPS PUB) 46, 1977.

[3] Shoji Miyaguchi, *The FEAL Cipher Family*. Advances in Cryptology – Crypto '90 Proceedings. LNCS 537, Springer, Berlin, 1991, pp. 627 - 638.

[4] X. Lai, J. L. Massey and S. Murphy, *Markov Ciphers and Differential Cryptoanalysis*. Advances in Cryptology – EUROCRYPT '91. Proceedings. LNCS 547, pp. 17 - 38, Springer, Berlin, 1991.

[5] International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), *B-ISDN ATM Adaptation Layer (AAL) Specification*. Recommendation I.363, 1993.

[6] International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), *B-ISDN User-Network Interface – Physical Layer Specification*. Recommendation I.432, 1993.

[7] Andreas Rieke and Hans-Jürgen Zepernick, *On Header Forward Error Control in ATM Systems*. Proceedings of the 4th UK/Australian International Symposium on DSP for Communication Systems, Perth, West Australia, Sep. 23 - 26, 1996.

[8] Daniel Stevenson, Nathan Hillery, Greg Byrd, *Secure Communications in ATM Networks*. Communications of the ACM, Feb. 1995/Vol. 38, No. 2, pp. 45 - 52.