Link Encryption in ATM Systems

Andreas Rieke
Forschungsinstitut für Telekommunikation (FTK)
Martin-Schmeißer-Weg 4, 44227 Dortmund, Germany
Tel.: ++49 2331/987-4331, Fax: ++49 2331/337789
E-mail: andreas.rieke@fernuni-hagen.de

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 with 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.

Keywords

Encryption, ATM, error multiplication, synchronisation

1 INTRODUCTION

Data encryption is required to provide privacy in communication channels and links, as in the Asynchronous Transfer Mode (ATM). Amongst different encryption techniques, only 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, fault tolerance and implementation will be discussed in detail.

In section 2, different modes of operation for encryption are shortly reviewed, before their relevant characteristics are referred to ATM systems. Section 3 gives a summary of current activities concerning encryption in the ATM Forum. In section 4, a cell payload encryption system is proposed.

If only the payload of ATM cells is encrypted, the header is transparent to an aggressor. It is possible to recognise how many virtual connections are in use; for each virtual connection, characteristics as mean bit rate and maximum bit rate can give information on the service that is being used. Active attacks like deleting single cells and inserting idle cells, instead, are possible.

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 5. Some concluding remarks are given in section 6.

2 MODES OF OPERATION FOR ENCRYPTION

Encryption functions can be classified in either block- or stream ciphers. Block ciphers are designed to encrypt a block of bits (usually 64 bits per block, but sometimes even more) simultaneously, whereas stream ciphers work on single bits or bytes, respectively.

Block ciphers are used in different modes of operation. Amongst these, electronic codebook (ECB) mode and cipher block chaining (CBC) mode are the only basic modes that match the definition of block ciphers.

For stream ciphers, two modes of operation are in use, too. In both modes, synchronisation between encryption- and decryption function is needed in order to gain the correct plaintext after decryption. The self-synchronising stream cipher is able to reach synchronisation automatically, whereas the synchronous stream cipher is not.

Block ciphers can also be used as keystream generators in both stream modes. In these cases, the modes of operation are called cipher feedback (CFB) mode for self-synchronising stream ciphers and output feedback (OFB) mode for synchronous stream ciphers.

The four basic modes of operation differ significantly in characteristics like cryptographic synchronisation, fault tolerance, implementation and security. Since the general differences are well known, only cryptographic synchronisation and implementation are concerned in the following because these characteristics have a special importance in ATM systems.

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

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. The cell delineation function extracts ATM cells from the incoming bit stream at the receiving side.

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.

Another important topic is encryption/decryption speed. The fastest hardware implementation of a block encryption system known to the author is a DES (data encryption standard) cipher (U. S. Department of Commerce, National Bureau of Standards 1977); its maximum speed is 1 Gbit/s (Eberle 1993). Thus, a single chip is able to encrypt one direction of a 622.080 Mbit/s link with low delay.

3 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 (ATM Forum 1996) 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 with a 56 bit effective key, Triple DES with a 112 bit effective key and FEAL (Miyaguchi 1991) 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 OFB; for this reason, resynchronisation algorithms are specified in this mode of operation. IDEA (international data encryption algorithm, (Lai *et al.* 1991)) is not (yet) specified for user plane data confidentiality.

4 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 a cell makes no problem at the sending side.

Assume that a cipher that requires cryptographic synchronisation is used. When sending a cell that must not be encrypted, the sending node could either stop the ciphering of this cell or continue without encrypting. As long as the receiving node acts in the same way and no errors occur, the system operates properly. But if an error like cell discarding occurs in the first case, the receiving node does not know whether to stop the cipher or not. For this reason, both ciphers must continue running even if no encryption or decryption takes place.

Therefore, cryptographic synchronisation is guaranteed as long as the cell delineation function works synchronously.

The cell payload is processed in the ATM adaptation layer (AAL). Due to different classes of service, different AALs are defined. 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.

A detailed analysis of the performance of AAL 1 in case of independent bit errors is given in appendix A. It is shown that link encryption with a cipher that causes error multiplication significantly reduces the performance compared to the not encrypting system.

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 (ITU-T: I.363 1993). Therefore, a single bit error in the not encrypting system can be detected reliably.

Since the number 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.

5 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 (ITU-T: I.432 1993, 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 (Rieke and Zepernick 1996).

In order to decide which mode of operation is more suitable for a complete cell encryption function, an analysis on effects of bit errors is performed in appendix B. The results of the analysis show that error multiplication considerably reduces the performance of the system.

Therefore, the synchronous stream cipher is the best choice in this case, too.

Again, 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.

6 CONCLUSIONS

It is not admissible to compare the ATM forum encryption scheme or other schemes like (Stevenson *et al.* 1995) 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.

Thus, undetected cell loss is possible and only self-synchronising ciphers can be used. Encryption of the ATM header is not possible because the cell header is processed by intermediate switches.

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

7 APPENDIX A

In all modes of operation except the synchronous stream cipher, bit error multiplication occurs. In this appendix, it is assumed that a single bit error in the ciphertext leads to a block of length l of random bits after decryption, where an integer multiple of l results in the cell payload length.

It is assumed that only the payload of ATM cells is encrypted. This payload is processed by the AAL. As an example, the performance of the AAL 1 segmentation and reassembly (SAR) sublayer and lower layers is analysed and compared to the not encrypting system. For the analysis, a transparent transmission system is assumed. That means, scrambling and coding techniques that also lead to error multiplication are not considered.

AAL 1 is constructed to transfer service data units (SDU) with a constant bit rate. In order to recognise missing or misinserted cells, a sequence number (SN) is placed in the SAR-PDU (protocol data unit) of AAL 1. The SAR-PDU format is shown in Figure 1.

The AAL 1 SAR sublayer supplies the convergence sublayer (CS) with three kinds of information:

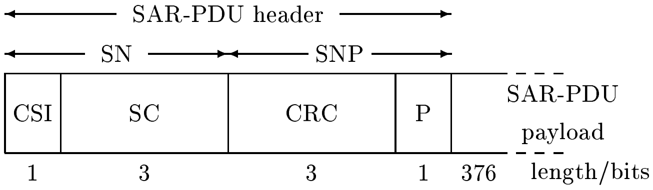

Figure 1 SAR-PDU format of AAL 1.

SAR:	segmentation and reassembly	PDU:	protocol data unit
SNP:	sequence number protection	SN:	sequence number
CSI:	convergence sublayer indication	SC:	sequence count
CRC:	cyclic redundancy check	P:	parity

- the AAL 1 SAR PDU payload,
- the sequence number (containing a sequence count and a CSI bit) and
- a status bit.

The status bit indicates whether the sequence number is invalid or seems to be valid.

The following two parameters are used to describe the performance of the AAL 1 SAR and lower sublayers:

E**:** average number of bit errors in the SAR-PDU payload and
H**:** probability of wrong sequence number or invalid status.

With a bit error probability P_{bit} the average number of bit errors in the SAR-PDU payload without encryption is

$$E_{normal} = 376\, P_{bit}. \tag{1}$$

With block encryption, bit errors in the block cause an average of $l/2$ bit errors after decryption. The probability of block errors is $P_{block} = 1 - (1 - P_{bit})^l \approx l\, P_{bit}$. The average number of bit errors in the SAR-PDU payload results in

$$E_{block} = \frac{1}{2}\left[l - 8 + l\left(\frac{384}{l} - 1\right)\right] P_{block} \approx 188\, l\, P_{bit}. \tag{2}$$

A bit error multiplication factor α can be defined by:

$$\alpha = \frac{E_{block}}{E_{normal}} \approx \frac{l}{2}. \tag{3}$$

When analysing the probability of a wrong sequence number or invalid status, it is assumed that the AAL 1 SAR works in correction mode. In correction mode, a single bit error in the SAR PDU header can be corrected. In case of additional errors, a wrong sequence number is generated or the status is invalid. The probability of a wrong sequence number or an invalid status without encryption is

$$H_{normal} = 1 - (1 - P_{bit})^8 - 8\,P_{bit}\,(1 - P_{bit})^7 \approx 28\,P_{bit}^2. \tag{4}$$

With block encryption, the first block carries random bits in case of one or more bit errors. In 9 of 256 cases the correct SN and status are generated; the probability of wrong information is

$$H_{block} = \frac{256 - 9}{256} P_{block} \approx \frac{247\,l\,P_{bit}}{256}. \tag{5}$$

The quotient of both probabilities is

$$\beta = \frac{H_{block}}{H_{normal}} \approx \frac{247\,l}{7168\,P_{bit}}. \tag{6}$$

Figure 2 shows the influence of error multiplication on AAL 1 SAR and lower layers performance.

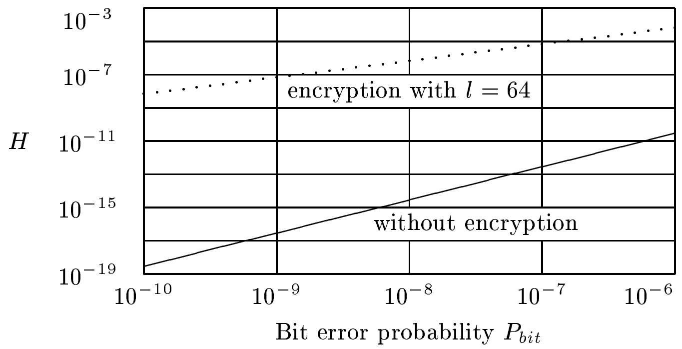

Figure 2 Influence of error multiplication on AAL 1 SAR and lower layers performance.
H: probability of wrong sequence number or invalid status

The analysis shows that link encryption with error multiplication changes the performance of AAL 1 SAR and lower layers in a significant way. AAL 1 SAR is constructed to handle single bit errors, but not block errors. For this reason, synchronous stream ciphers are more suitable for cell payload encryption.

8 APPENDIX B

This appendix deals with the effects of bit errors in the encrypted data stream in case of complete cell encryption. As described in section 5, the cell payload and header without HEC are encrypted, in order to compute the HEC from the encrypted header at the sending node. 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.

Thus, the self-synchronising cipher is analysed. It is assumed that single bits are processed without interleaving. The case of parallel processing leads to similar results and is not considered in this paper.

The number of bits of the internal state is denoted l. For practical reasons, it is sufficient to consider $32 \leq l \leq 384$ in the following analysis, but the results are also given for $1 \leq l \leq 416$.

In case of cell discarding, the internal state of the cipher which is used to decrypt the next cell is not known; thus, the next cell can not be decrypted and is only used to update the internal state.

In case of a single bit error, it is assumed that cell i is hit at position x. For $0 \leq x < 40$, the error occurs in the header; assuming correction mode, the error is corrected,

$$P_{i+1,correct,1} = \frac{40}{424}. \tag{7}$$

For $40 \leq x < 424$, the error occurs in the payload, and leads to a payload error of cell i both with or without encryption.

Thus, encryption with a self-synchronising cipher does not lead to different error probabilities in cell i. But without encryption, the cell $i + 1$ is not concerned by an error in cell i, whereas with encryption, it is.

The following analysis will show the probabilities for the cell $i + 1$ to be correct ($P_{i+1,correct}$), to contain header errors ($P_{i+1,header}$) and to contain no header errors, but payload errors ($P_{i+1,payload}$).

When the error occurs in the payload of cell i ($40 \leq x < 424$), it is easier to view the process after header sequence generation/verification.

Since the cell header is free of errors in this case, the HEC field may simply be omitted. The payload is now located at $32 \leq y < 416$. Figure 3 shows the ATM cell format at the header sequence generation/verification and link encryption function.

An error in the cell payload at position y leads to l random bits, starting at position $y + 1$. This burst does not lead to an error in cell $i + 1$ if $32 \leq y \leq 415 - l$,

$$P_{i+1,correct,2} = \frac{1}{424} \sum_{y=32}^{415-l} 1 = \frac{384 - l}{424}. \tag{8}$$

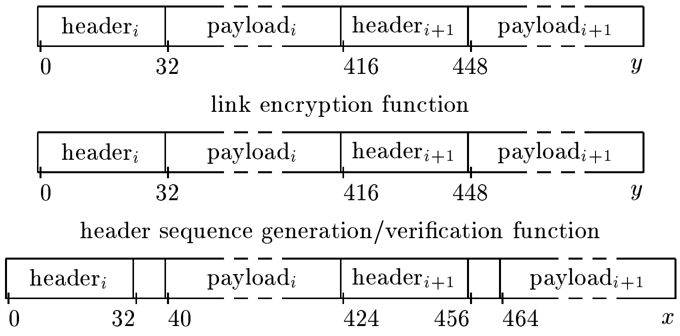

Figure 3 ATM cell format at the header sequence generation/verification and link encryption function.

The burst reaches to the header of cell $i+1$ if $416-l \leq y \leq 447-l$. In this case, $b = y + l - 415$ bits of the burst affect the header of cell $i+1$. If none of the random b bits leads to an error, the next cell is correct,

$$P_{i+1,correct,3} = \frac{1}{424} \sum_{y=416-l}^{447-l} 2^{415-y-l} \approx \frac{1}{424}. \tag{9}$$

In the other case, cell $i+1$ has a header error,

$$P_{i+1,header,1} = \frac{1}{424} \sum_{y=416-l}^{447-l} \left(1 - 2^{415-y-l}\right) \approx \frac{31}{424}. \tag{10}$$

The last case is given when the burst reaches to the payload of the next cell. Taking $448-l \leq y \leq 415$, all 32 bits of the header of cell $i+1$ are affected, additionally $b = y + l - 447$ bits of the payload. Cell $i+1$ is correct with the neglectable probability

$$P_{i+1,correct,4} = \frac{1}{424} \sum_{y=448-l}^{415} 2^{415-y-l} \approx 0. \tag{11}$$

Payload errors of cell $i+1$ are also neglectable; they occur with the probability of

$$P_{i+1,payload} = \frac{2^{-32}}{424} \sum_{y=448-l}^{415} \left(1 - 2^{447-y-l}\right) \approx 0. \tag{12}$$

A header error may also occur with

$$P_{i+1,header,2} = \frac{1}{424} \sum_{y=448-l}^{415} \left(1-2^{-32}\right) = \frac{\left(1-2^{-32}\right)(l-32)}{424} \approx \frac{l-32}{424}. \quad (13)$$

A summary of the results

$$P_{i+1,correct} = \sum_{j=1}^{4} P_{i+1,correct,j} \quad (14)$$

$$P_{i+1,header} = \sum_{j=1}^{2} P_{i+1,header,j} \quad (15)$$

leads to

$$P_{i+1,correct} \approx \frac{425-l}{424} \quad (16)$$

$$P_{i+1,payload} \approx 0 \quad (17)$$

$$P_{i+1,header} \approx \frac{l-1}{424}. \quad (18)$$

The results, which are also given in graphical form in Figure 4, show that single bit errors lead to header errors with high probability in case of self-synchronising stream ciphers. For that reason, only synchronous stream ciphers are suited for complete cell encryption in ATM systems.

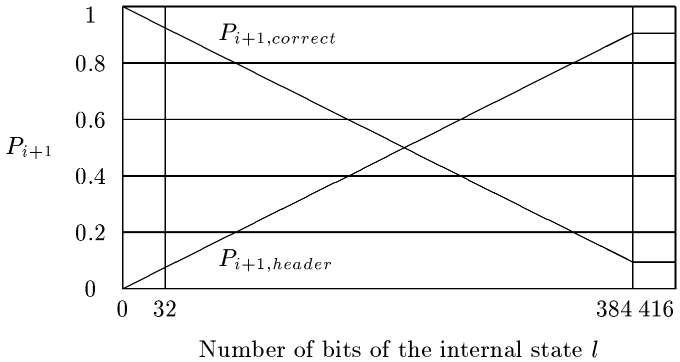

Figure 4 Effects of a single bit error in cell i using a self-synchronising stream cipher.

9 REFERENCES

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

Hans Eberle, *A High-speed DES Implementation for Network Applications*. Advances in Cryptology – CRYPTO '92. LNCS 740, Springer, Berlin, 1993. pp. 521 - 539.

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

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

Xuejia Lai, James L. Massey and Sean Murphy, *Markov Ciphers and Differential Cryptanalysis*. Advances in Cryptology – EUROCRYPT '91. LNCS 547, Springer, Berlin, 1991. pp. 17 - 38.

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

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

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.

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

10 BIOGRAPHY

Andreas Rieke received the degrees Dipl.-Ing. (FH) in 1990 and Dipl.-Ing. in 1993 from the College of Bielefeld, Germany and the University of Hagen, Germany, respectively. From 1991 until 1992, he worked in the Laboratory for Applied Mathematics at the College of Bielefeld. From 1993 until 1994, he was at the University of Hagen as Research Assistant. Since 1995, he has been with the Forschungsinstitut für Telekommunikation, Dortmund, Germany, and is currently working on his Ph. D. thesis. His present research interests include applications of security functions and error control techniques in ATM systems.