SECURITY MECHANISMS FOR ATM PONS

S. Velentzas, H. Cruickshank, Z. Sun, G. Pavlou
Centre for Communications Systems Research
University of Surrey, UK

ABSTRACT

Widespread acceptability of B-ISDN will be achieved only if broadband services are attractive not only to business, but also to the residential and small business customers. Although, these customers’ demands for the new broadband services have been steadily increasing, their decision on joining the world of broadband networks depend mostly on the access cost. A disadvantage of dedicated fiber local loops is the expensive installation cost. This led to the development of Passive Optical Networks (PONs) for access to broadband services.

The passive splitting of optical signals, which gives flexibility, low cost and robustness, creates a broadcast architecture undesirable in public access networks. Providing security mechanisms for ATM PONs will make viable an ATM solution up to the residential users, providing them with secure high bandwidth data sensitive applications i.e. home shopping, banking, video on demand, etc. Demonstrating the protection and security achievement for the services to residential users is mission-critical for the PONs concept to succeed.

The purpose of proposed telecommunication security is to protect the network’s resources and information transmitted over the PONs through the selection and application of appropriate safeguards i.e. public key cryptography, digital signature, certification authorities, time-stamping, key generation and personalisation, etc. A secure, robust protocol is needed which will be able to provide the flexibility that different access networks require and the security mechanisms that will guarantee authentication, confidentiality and integrity.

1. INTRODUCTION

1.1 RESIDENTIAL MARKET

The market situation in telecommunications around the year 2000 and beyond will be dominated in most European and other industrial countries by a deregulated Telecommunication Market and highest competition between old and new operators, as well as new service providers.

Key market segments of competition will be terrestrial and mobile telephony and all kinds of data services, with particular emphasis on tele-banking and Internet services. New local and mobile terminals will offer an integration of comfort and service tailored functionality to subscribers and especially to the residential users who constitute a virgin market, until now. A forecast of expenditures on telecommunication products and services for the residential and small business market is presented in Figure 1.

The implementation of interactive broadband access networks will provide major opportunities for marketing new products, offering its capabilities to residential consumers i.e. households and businesses. The services and capabilities specified for ATM Residential Access networks are similar to those specified for other ATM networks. Network operators may elect to offer, and equipment in the home may be elected to be used if offered, all or a subset of broadband residential services and capabilities. It is intended that seamless inter-operation will be possible between ATM end-systems attached to residential broadband networks and ATM end-systems attached to other ATM networks.

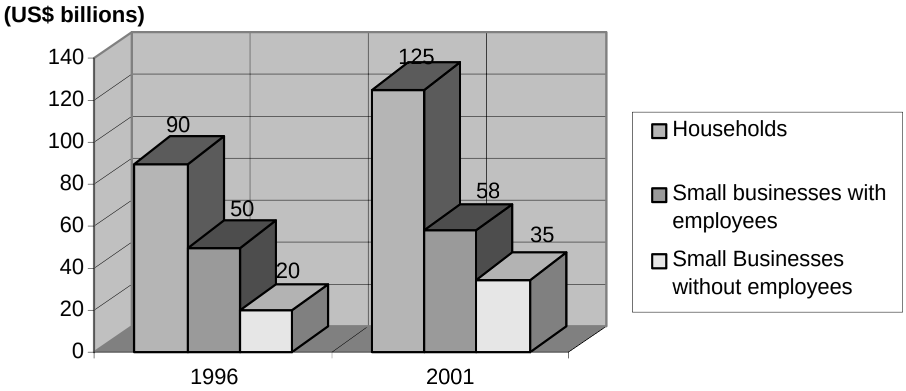

Figure 1: Residential and Small Business Market Expenditures [Insight Research]

1.2 ACCESS TECHNOLOGIES

There are different varieties of access networks due to local regulatory, geographic, installed infrastructure constraints (i.e. cable TV, telephone wiring), etc. Figure 2 illustrates these approaches and the Table 1 provides a brief technical comparison between most of them. The security mechanisms proposed can be applied to most of these cases but it will be concentrated on the ATM technology, considering Fiber To The Curb (FTTC) and Fiber To The Home (FTH) scenarios.

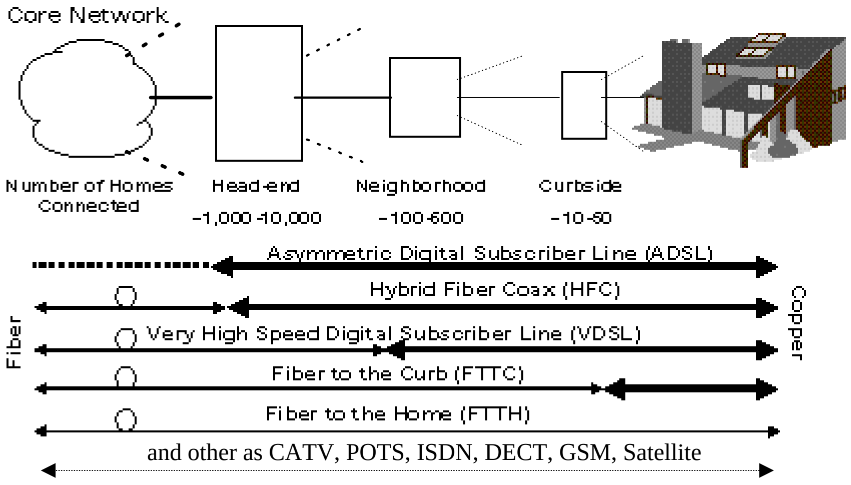
Core Network
Number of Homes Connected
Head-end
~1,000-10,000
Neighborhood
~100-600
Curbside
~10-60
Asymmetric Digital Subscriber Line (ADSL)
Hybrid Fiber Coax (HFC)
Very High Speed Digital Subscriber Line (VDSL)
Fiber to the Curb (FTTC)
Fiber to the Home (FTTH)
Fiber
Copper
and other as CATV, POTS, ISDN, DECT, GSM, Satellite

Figure 2: Access Network Configuration

The access network delivers services over ATM to the home network, which distributes the service throughout the residence. It allows multiple service providers (e.g. cable, telephone, utility companies) to connect to a single home network and broadband appliances in the house (e.g. Digital VCR, HDTV, PCs, Digital Set-Top Boxes) to be interconnected.

Technology	Downstream Rate (Mbps)	Upstream Rate (Mbps)	Wire Distance (maximum)	Homes per Neighbourhood
FTTH	155	155	not applicable	10 to 200
FFTC	25 - 50	25 - 50	100 m	10 to 50
VDSL	13 - 60	1.6 - 5.0	2 Km	100
HFC	45*	1.5*	not applicable	500
ADSL	1.5, 6	64, 640	4, 6 Km	1,000 - 10,000

Table 1: A Comparison of Access Approaches
(* signifies shared bandwidth)

1.3 STANDARDISATION EFFORTS

ATM Forum can be considered as the most significant standardisation effort on the ATM access networks. A technical document is expected to be released from ATM Forum Residential Broad Band Group (RBB) by end of 1998 summer but there are provisions or considerations in respect with the security compromises that exist in the access networks. It is strongly believed that until security mechanisms and sufficient (or mathematical) proof are provided, the access networks and especially PONs, will not be able to penetrate to the residential market supporting the long awaited services with high bandwidth. The defined ATM RBB access technologies are illustrated in the Figure 3 [1].

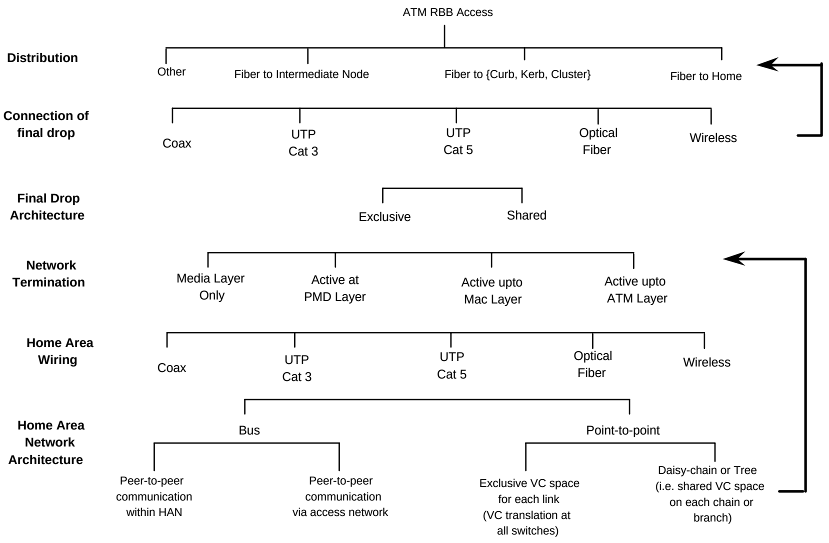

Figure 3: ATM RBB Access Technologies [ATM Forum]

1.4 IDENTIFICATION OF THE AREA OF INTEREST

Figure 4 illustrates the reference architecture which provides an identification of the ATM interfaces and a representation of the access network targeted by this paper. The generic ATM reference architecture is consisted of the following elements: core ATM Network, ATM access network, access network termination, home network (could be ATM) and terminal equipment.

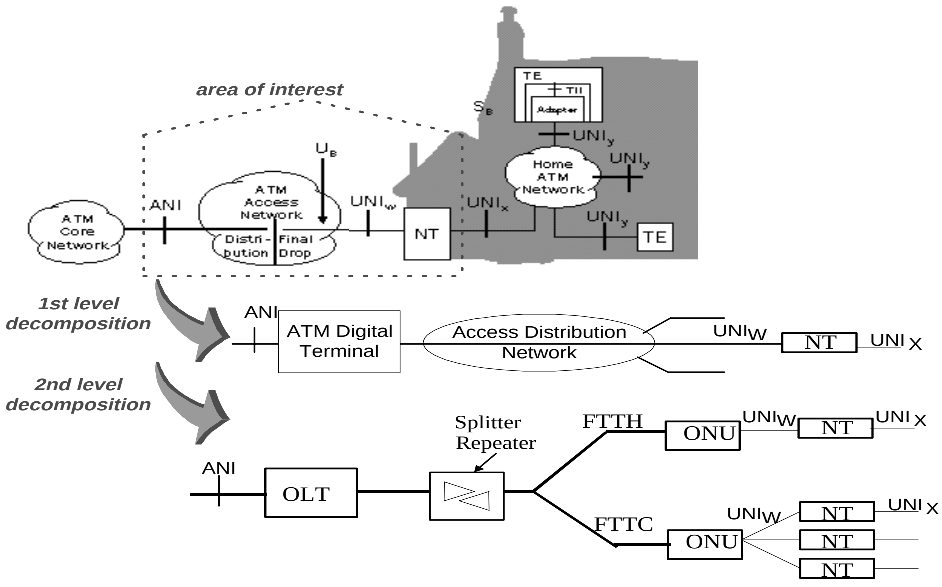

Figure 4: Reference Architecture

The PONs considered are the ones with a tree-like architecture i.e. the root of the tree positioned in a central place and the terminals (leafs) scattered. The trunk and the main brunches of the network are consisted of optical fibres common to all users and only the last drop is dedicated.

PONs are starting to be deployed in the access network with main reasons the (1) *economics*, rapidly declining cost of fibre optics, simpler network engineering, and lower operational and maintenance costs, and (2) *strategic*, future proofing of the access network since it can support narrowband and broadband services.

The objective of the photonic access network is to define and develop a cost-effective full-service optical access network, anticipating the needs and new developments in the telecommunications industry. The introduction of new services is expected to create a large increase of traffic flow which must be accompanied without significant increase of the access cost. The increased capability must be accompanied by greater flexibility in the exploitation of resources allowing sharing of infrastructure and cost.

The goal of the paper is to define a complete end-to-end secure system, for a variety of services over a variety of systems (but illustrating that over ATM), to and from the residential site. The emphasis of this effort is to identify the appropriate interfaces and signalling, complying to existing and emerging ATM Forum specifications, and standards from other bodies and present security mechanisms that are believed to be able to counteract the current imposed threats, concentrating on the ATM PONs access networks.

It is needed to clarify that the access network termination is a functional grouping that connects the ATM access network to the home ATM network and that a NT may be either passive or active. UNI_W is the interface at the access network side of the NT and UNI_X is the interface at the home side of the NT. In the case of a passive NT, the UNI_W and UNI_X interfaces are the same but here an active NT is considered i.e Layer 1 functions, such as modulation and demodulation, active components, such as a bridge at the Media Access Control, Transmission Convergence sublayer, an ATM switch or a multiplexer at the ATM layer. The physical device which contains the NT may also contain other functions which this is the case within this paper.

2. PONs SECURITY COMPROMISES

The broadcast downstream topology of PONs, results in a loss of privacy in comparison with the star of the point-to-point fiber links. This privacy should be restored by means of encryption. The critical issue are to identify the specific PON threats and to define at what level to introduce the needed security mechanisms.

If all services were encrypted at the application level, then there maybe no high need to introduce extra (i.e. network) encryption, depending on the kind of services that will be supported/provided. On the other hand, at least for the first years of PONs (or residential broadband services) deployment, many services will not possess an application level security. A security mechanism introduced in the lower layers of the OSI protocol stack will be required or at least a combination of lower and higher layer security. It should be noted that the low layer security is preferable in most cases due to performance and time considerations.

2.1 THREATS IDENTIFICATION

Threats can be seen as *potential violations of security,* with expected or unexpected harmful results, and exist because of vulnerabilities in a system. The threats explained in this section are specific to ATM PONs. There are several other threats that can compromise the security of the ATM PON but these threats are generic and can be applied in any other communication system and can be identified by literature survey.

For the PONs, several specific problems could arise that make the network insecure. Measures addressing these specific threats should be taken for securing the communication transfer over the access network. The peculiarities of PONs can be summarized as:

- Downstream data is broadcasted
- Sharing of the same upstream medium
- Insecure access to the common medium and traffic regulation

On downstream, each user has the straightforward opportunity to exercise some of the general communications threats. The attacker does not make any significant effort in obtaining data destined for others, as it is delivered to any user's device. Therefore, a legal protection scheme is impossible to be efficiently exercised, without an introduction of a security mechanism.

On upstream, an attacker has the opportunity to easily intervene, disrupt and modify others data. The threats are arising from this peculiarity do not exist generally in other networks. The access of the common medium and the regulation of traffic are based on information given by the users. This means that a malicious user has the opportunity to cause a number of problems, not only to individual users but also to the whole network. It should be noted that it is useful to distinguish between upstream and downstream directions and identify specific threats.

2.1.1 Upstream

Specifically for the upstream direction, reflections at the power splitters do not lead to readable information. Therefore, eavesdropping on upstream information is not a problem. The real concerns are authentication and data integrity. A malicious user can impersonate an authorised subscriber in two ways:

- *Impersonation*. The OLT has no way of detecting if some user is presenting himself as another user. Therefore, impersonation is a serious threat and can lead to several security problems. For example, an attacker sends information (i.e. in cells) with a VPI/VCI of another subscriber in his own allocated time-slot. This way, it generates unwanted information in another connection. Measures should be taken to protect the impersonation from other users.
- *Data integrity*. In the case that some user tries intentionally to modify or disrupt the data sent by another user actions should be taken to locate the intruder. Since there is no means to prevent or exclude such cases, effort should focus in rapid location and punishment of the intruder. For example, a malicious user sends information at the same time as the authorised subscriber. As the receiver at the OLT has to cope with different power levels, it might be possible to completely overwrite the correct information by sending at a higher power level. In contrast, transmission at the normal power level would typically produce a corrupted cell (loss of data integrity) which may or may not be detected by the application.

2.1.2 Downstream

On the other hand, on the downstream direction the OLT broadcasts the information to all ONUs and therefore eavesdropping is possible. This is one of the main security compromises for the ATM PONs, which is also identified in LANs which support broadcast / multicast services due to their shared-medium LAN features. This problem applies to permits, OAM addresses, OAM commands, and the downstream ATM cells containing signalling information, user data, or OAM information. The threats arising from the broadcasting in the downstream direction can be classified as:

- *Eavesdropping of ATM cells payload*. Every user can eavesdrop the data of other users. If the data is not encrypted, this is a violation to the confidentiality principle. This is a major threat and can be faced by encryption of the ATM cells payload.

- *Eavesdropping of the OAM cells.* The OAM ATM cells generated within the network should be encrypted. This is necessary because the users of the network can interpret them and gain information about traffic and routing data of other users.

Therefore, the intruder may collect information about:

- The amount of traffic generated and received by a subscriber which is derived from permits and VPI addresses.
- The communication partners of a subscriber, which are derived from signalling information.
- The user, which is derived from the payload of ordinary packets (i.e. ATM cells).
- Management policies and internal states of the system, which are derived from OAM cells and fast OAM commands.

3. PROPOSED SOLUTION

3.1 SECURITY MECHANISM AT HIGHER LAYERS

The security mechanism suggested is going to be based on the application of hybrid cryptosystems i.e. exchange of session keys by using the public key cryptography. The proposed security protocol is illustrated at Figure 5, where with the originated SETUP message, the user's (residence or a Small Office Home Office - SOHO) public key is also forwarded with an indication of the supported encryption algorithms. The received user, selects a supported encryption algorithm, generates a session key, which is frequently changed during the established communication, signs with the user's private key, attaches the user's public key and encrypts with the received public key. This information is sent back to the originating user with the CONNECT message.

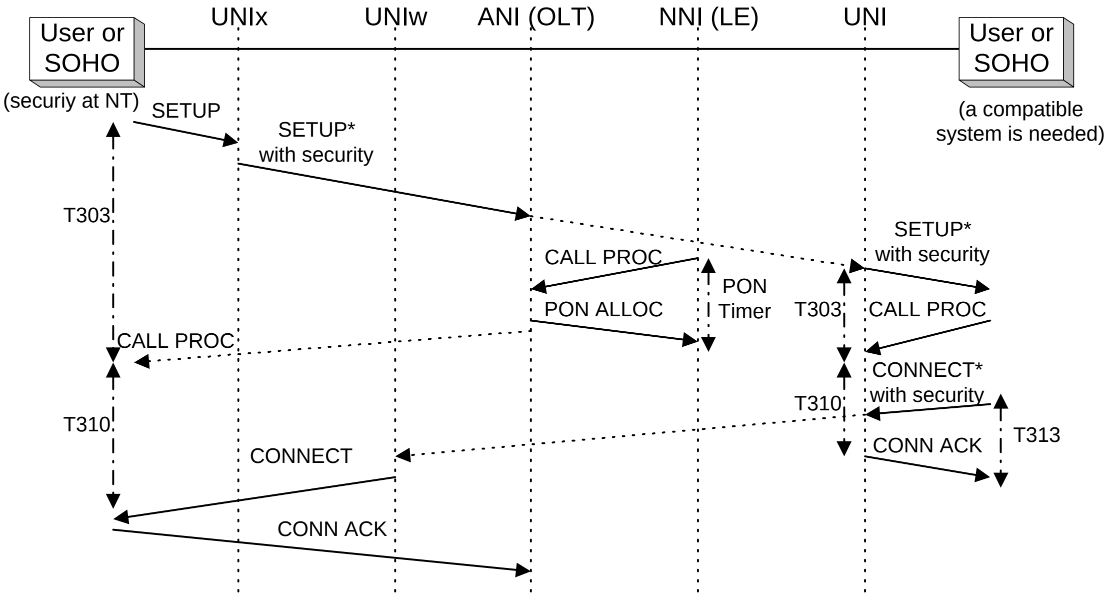

Figure 5: Secure Protocol Over an ATM PON.

It should be noted that this mechanism can present potential weaknesses against potential attacks with re-sending recorded legitimate messages. For this reason, the measures taken to counteract these potential attacks are different encryption algorithms for the encryption and signing of the message. Further to that time-stamping can be employed, but only combined with the usage of different algorithms, since it is considered troublesome in respect with time issues.

This is a secure communication that can be established between two end parties but presents the weakness of another legitimate user impersonating the originating user with the call setup message i.e. forwarding the user's public key. This can be performed by intercepting the call setup and forwarding to the recipient user, a new call setup with the interceptor's signature and public key. This way when the recipient user replies with the session key (and recipient's public key, etc.), the interceptor will be able to decode them and establish a communication with the recipient, succeeding to impersonate the originating user. In the case of services, the interceptor will be able to get access to the provided services.

The problem lies in the secure delivery of the initiator's public key. This security compromise together with the threats described in section two, necessitates the introduction of additional (or low layer) secure mechanisms. Figure 6 presents the new suggested architecture with the introduction of more security mechanisms at a hardware level and taking under consideration and supporting the telecommunications trends for providing residential gateways, as complex modular interworking devices, being used at different access networks as presented at Figure 2. The only other way that the same security result could be achieved is believed to be with the employment of certification authorities and/or trusted third parties. This solution was avoided as they were considered to introduce unnecessary complexity and overhead, which can be saved with the hardware solution.

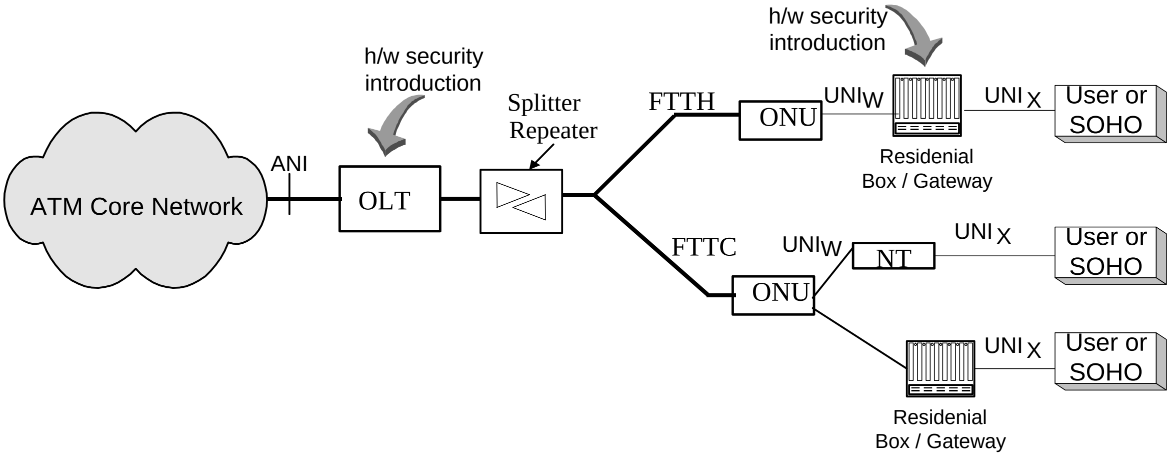

Figure 6: Revised Secure Protocol over an ATM PON.

The suggested security mechanisms outlined in Figure 5, will be introduced above the ATM Adaptation Layer (AAL) for supporting end-to-end secure communication. It will not burden the ATM network with unnecessary functionality as only the user payload will be encrypted. It will not impose an overhead on performance and additional complexity on the ATM switches of the core network for decrypting (and then encrypting) the cell header for routing purposes. An AAL level encryption would also complicate the AAL operations, since there are several types of AAL, such as AAL1, AAL2, AAL3/4 and AAL5 (and there may be more in the future) and some AAL layers check for transmission errors using Cyclic Redundancy Check i.e. encrypting the CRC field makes it difficult to distinguish between a transmission error and security breach.

3.2 ADDITIONAL HARDWARE SECURITY

The additional hardware security described in Figure 6, which presents the introduction of hardware modules at the residential site and the OLT, will secure the ATM PON access network and provide the benefits of fast encryption and decryption. The introduction of security hardware modules always bring in mind non-flexibility, dependency to the manufacturer/provider of the hardware module, non-ability to securely communicate with other users of not comprising the same module, non-confidence to the hardware storage of the keys, etc. These issues do not apply to the proposed module since:

- The hardware implementation should be in a modular form, easily to be incorporated both at the Residential Box/Gateway and the OLT. In that way, it will provide ease of maintenance and upgrade.
- Indeed, the implementation of the hardware module will be manufacturer/provider dependent and it could be a total hardware or software/hardware implementation. On the other hand, the implementation will support most of the standard encryption algorithms, and multiple key lengths and therefore it will not present a communication problem between users with different manufacturer's security modules.
- The security module will store in a secure, hardware oriented and non-recoverable way the private key(s). This requirement is not of high importance for the residential module, since it is situated in a relevant protective and secure environment, but it is important for the secure module at the OLT.
- Plug and Play principles will be supported for the security module, enabling direct integration within both the residential box and OLT i.e. do not disturb the OLT and residential box operation, definition of communication interfaces between the hardware modules, etc.
- Existence of uniformity between the higher layer security mechanisms and the hardware coded security mechanisms of the security module i.e. application of hybrid cryptosystems. This will provide the ability of the security module usage (whenever appropriate) by the higher layers security mechanisms described in the previous section.
- Utilisation of the hardware module for the provision of other mechanisms that could be proven useful to the user and network i.e. implementation of hardware compression before transmission of information.

The operation of the hardware module will be similar to the operation of the higher layers mechanisms but it will not be needed to insecurely forward the residential user's public key. This is because the public key of the OLT will be delivered to the residential user securely, enabling him to generate a session key (which will be frequently changed between the ONU and the residential box / gateway), include an indication of the supported encryption algorithms (needed only to be performed the first time for selecting an encryption algorithm with the OLT and then rarely), sign with the user's private key, attaches a timestamp and the user's public key and encrypts with the securely known OLT public key. Upon reception of this encrypted information, the OLT manages to decrypt it by using its private key, authenticates the residential user (signature and timestamp), and performs future communication with the residential user by encrypting the information using the proposed session key (and timestamping). From the OLT point of the network, the information can securely propagate over the core network according to the way described in the "Securing User, Control and Management Planes in ATM" paper [2] or according to ATM Forum's suggestions [3].

The security module will exhibit the following features that will resolve the impersonation problem with the public key:

- When the security module is being plugged/integrated at the OLT, it will automatically produce a pair of keys (public and private) to be used from then onwards. Provisions for updating/changing these keys will exist but it is needed to securely update all residential boxes if the public key is changed.
- When the security module is being plugged/integrated at the residential box / gateway, it will be requested to provide the OLT public key. This key is made known via the access network provider at the connection of the residential box / gateway to the network or with the provision of the services and/or the security module. A pair of keys (public and private) will be automatically created and there should be provisions for updating/changing the key pair.

The threats discussed at section 2 can be addressed now, since there is no information non-encrypted that a potential intruder/attacker can access. Specifically, for the downstream direction the broadcasting feature of the ATM PON is now secured, since all the information is now encrypted and therefore eavesdropping is not possible. This applies to all information i.e. user data, ATM cells containing signalling information, OAM information, etc. An intruder can no longer collect information about the amount of traffic generated and received, the communication partners, the payload of ordinary packets of a subscriber and the management policies and internal states of the system. For the upstream, the situation is improved but still not totally resolved. It is not possible for an intruder to impersonate another user (i.e. digital signatures and timestamping). On the other hand, an intruder can still plug-in at an end-point of the access network and produce traffic with a total new pair of keys (public and private) and compromise the data integrity of the user and system. The timestamping and the digital signatures mechanisms make the identification of the problem by the OLT much easier and actions for locating the intruder and punishing him/her can be achieved.

4. CONCLUSIONS

The proposed security mechanisms described in the paper will increase operators, service providers and users confidence in ATM PONs technology and will accelerate the deployment of this type of access networks. Specifically, the paper's objectives were to:

- Present the need of residential users for higher bandwidth applications, briefly describe the diversity and variety of the access networks, identify the current standards status and outline the potential of ATM PONs.
- Define the vulnerable parts of the ATM PONs and assess the threats that may exploit them.
- Describe the proposed security mechanisms that can be employed to implement a secure communication over the access network and the core network.
- Explain their applicability in securing the previously identified threats to the ATM PONs.

This paper addressed different telecommunication aspects i.e. ATM PONs, residential box / gateway, identification and assessment of security compromises, and presentation of a proposed software/hardware solution, for achieving an end-to-end secure communication over ATM PONs access networks. An extended paper submission will be concentrated on the details of the proposed security mechanisms, their interworking and a proof that these mechanisms actually provide an adequate level of security.

REFERENCES

1. ATM Forum, RBB Baseline Document, Draft, ATM FORUM/98 -BTD-RBB-001.07, February 1998.
2. H. Cruickshank, Z. Sun, S. Velentzas, 1997, Securing User, Control and Management Planes in ATM, *SICON97*, April 14-17, 1997, Singapore.
3. ATM Forum, Phase I ATM Security Specification, ATM FORUM/95-1473R3, June 1996.
4. ETSI, Signalling Protocols and Switching, V Interfaces at the Digital Service Node, Identification of the applicability of existing protocol specifications for a V_B reference point in an access arrangement with Access Networks, version 1.5.
5. ATM Forum, Phase I ATM Security Specification, ATM FORUM/95-1473R3, June 1996.
6. Baum M., *Certification Authority Liability and Policy*, NIST-GCR-94-654, NTIS doc. no. PB94-191-202, 1994.
7. ETSI ETR/NA-002501, 6/11/1995, Security Technique Advisory Group (STAG) Security Requirements Capture.
8. Telematics Engineering/ICE-TEL Project, Architecture and General Specifications of the

Public Key Infrastructure, COST, September 1996.

9. ISO/IEC JTC 1/SC27 N691, Guidelines on the use and management of Trusted Third Party Services, August 1993.

10. Aggelopoulos, J.: Performance of shared medium access protocols for ATM traffic concentration, *EET, 5*, Special issues on Teletraffic Research for Broadband ISDN in the RACE programme, 1994.

11. Aggelopoulos, J.: Time division sharing of tree PONs by ATM users: A method to control cell jitter, *EUROPTO (SPIE/EOS)*, Conference on Broadband Strategies and Technologies for Local, Metropolitan and Optical Access Networks, Amsterdam, The Netherlands, March 1995.