A New Authentication Scheme for Wireless ATM Networks (WATM)

Hadj GHARIB, Nidal ABOUDAGGA and Aoued BOUKELIF

***Abstract**: Wireless ATM (Asynchronous Transfer Mode) network (WATM) like other wireless networks is vulnerable to security attacks because of its openness of transmission media. WATM network security is somewhat more concentrated and complex than that of wired ATM network. Authentication is the only sure method to ensure the proper use of service desired. However its limited resource, such as weak power supplies and limited bandwidth, must be taken into account in the design of security schemes. A user when roaming across networks must authenticate in each new visited network, but often the visited network may not be in a direct agreement with the user and must call the home network to ascertain the identity of the user and the nature of the service aimed to be shared with him. This procedure requires the intervention of the home network and time to authenticate for it depends on the response it engenders. In this paper, we present a new and efficient wireless authentication that provides fast seamless authenticated handover among WATM.*

***Key words**: authentication, roaming, security, wireless, WATM*

1. INTRODUCTION

The increasing need for high bandwidth exchanges in communication networks enhance the interest for ATM technology. ATM combines both data and multimedia information into the wired networks while scales well from backbones to the customer premises networks. The performance is due to the fact that ATM networks encapsulate their exchanges in fixed size cells of 53 bytes instead of packets. Wireless communication networks have been growing very fast in the last decade, which led us to think creatively of a solution for mobility in ATM networks through wireless ATM (WATM). WATM can be viewed as a solution for next generation communication networks. However, the WATM user, when roaming across different ATM networks, must authenticate at each newly visited network, even if the visited WATM does not share previously established security association with the visiting user. The security features for mobile communication system include: confidentiality on the air interface, anonymity of the user and most importantly, authentication of the user to the network in order to prevent fraudulent use of the system [1]. The goals of the authentications protocols typically include verifying that the identity of some party involved is the same as that claimed, and establishing a session key for use in conjunction with chosen cryptographic algorithms to secure the subsequent session. These goals are typically part but not all of what is needed for a secure mobile protocol in particular; there are additional factors that naturally arise due to the specific nature of the mobile environment [2]:

- Heterogeneous communications path like the radio link where it is very vulnerable to attacks.
- Location privacy the mobile station is allowed to roam freely and information on its location may be valuable to an adversary.
- Computational constraints of the mobile station and the terminal user.

This paper presents a new solution for secure roaming across WATM networks. In

section 2 we present the WATM architecture. A background of previous related works is given in section 3. In section 4 a new scheme of authentication is presented. Analysis on the proposed scheme and comparison of various protocols are given in section 5.

2. WATM ARCHITECTURE

2.1. Fundamental characteristics of ATM networks

ATM differs from all other networking strategies trough the combination of the following three characteristics:

- Fixed-size cells: all traffic-audio, video, or data is organized into fixed-length packets to permit greater efficiency in switching, from the hardware perspective, than for variable-length packets.
- Connection-oriented service: all of the cells of a given message are propagated along the same route that is established following a connection request and prior to launching the first traffic cell.
- Asynchronous multiplexing: To ensure fairness and efficient use of bandwidth resources, cells arriving at the input of any ATM switch, possibly from different users, are selected through statistical multiplexing, subject to priority considerations, and processed by the switch [3].

Due the success of ATM on wired network as board-band network which support all traffic, voice, data and video and the increasing importance of portable computing/telecommunications applications, wireless extensions to broad-band networks will be required to support user requirements. The basic idea is to provide a seamless wired and wireless networking environment with uniform protocols and application across both mobile and fixed devices [4]. A wireless ATM system consists of three major components with mobility support software to perform application adaptation management of QoS and mobility [5]. Fig.1.

1. ATM switches
2. Base stations

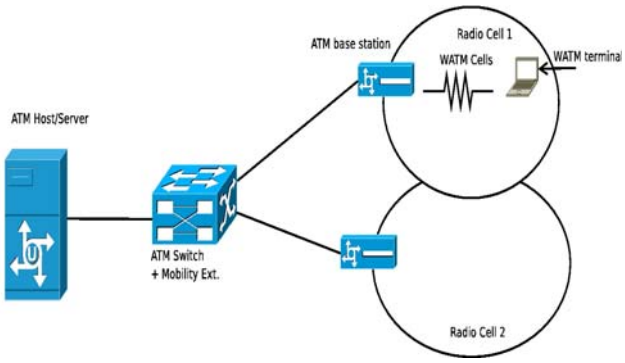

Fig. 1. WATM Network Components.

3. WATM terminal

3. RELATED WORKS

While working on wireless ATM networks, we have found very little work on the subject, including the work of D. Patiyoot et al. [6] This led us to pursue further research on the security of wireless networks in general. D. Patiyoot et al. presented seven proposals - TABLE I - for the security of WATM essentially based on the technique of public key and secret key. In his study he uses a third authority he calls WASA (Wireless Security Agent) and in another context WAAS (Wireless ATM Authentication Server) to authenticating the user in unknown area. It is obvious that the secret key solution made a huge gain in terms of time and energy consumption, but the increasing exchange of messages between entities is a weakness for strong and fast authentication. At the last D. Patiyoot et al., leave the field free to the choice of a mechanism and conclude that the choice may be influenced by the strength of the encryption, the computation time or more even the specific network resources.

Table 1. D. PATIYOOT et al. Authentication Protocols.

	Secret/Public key	Third Party
Session key	Public	Yes (WAS)
Secret Key	Secret	Yes (WASA)
Needham-Schroeder	Public	Yes (WASA)
Server	Secret	Yes (WAAS)
Otway-Rees	Secret	Yes (WAAS)
Carlsen	Secret	Yes (WAAS)
Kao Chow	Secret	Yes (WAAS)

4. PROPOSED ROAMING SCHEME

Our proposal is based on the idea of autonomous certificates proposed by M. Long et al. [7] and on the other hand on adaptation of TLS enhanced handshake protocol. fig. 2. Once the general-propose X.509 certificate structure has been criticized. fig. 3.

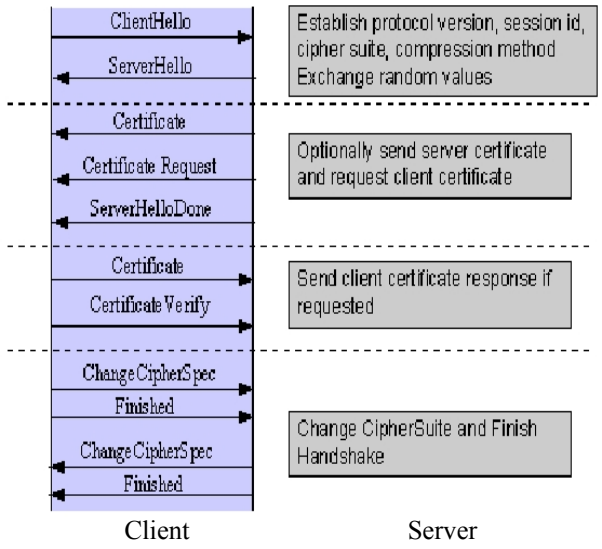

Fig. 2. Simplified Handshake Protocol.

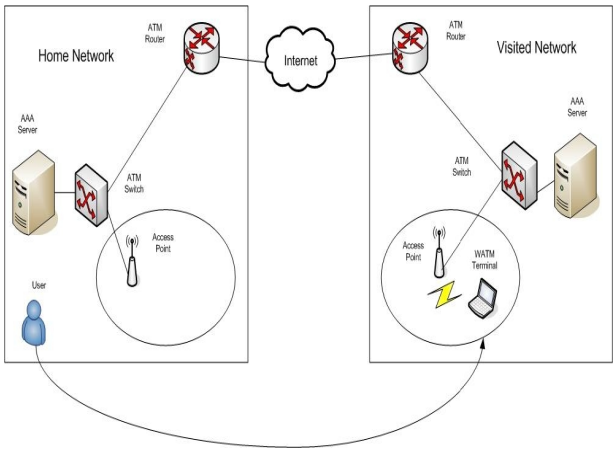

Fig. 3. Classical Roaming Scheme.

4.1. An overview of TLS

TLS is a transaction security standard providing secure connections between two communicating entities, with mutual authentication, integrity-protected security parameters negotiation and key management. It consists of several sub-protocols, especially Record and Handshake protocols. The first provides basic connection security for various higher layer protocols through encapsulation, whereas the second allows two entities to agree upon security parameters. The Handshake provides mutual authentication based on the use of certificates or pre-shared keys and instantiates negotiated security parameters and attributes for a session. These attributes include the cipher suite (the set of ciphers to be used in a session), the authentication method and the session Keys. The cipher suite is negotiated through the parameter 'CipherSuite list', which conveys the combinations of cryptographic algorithms supported by the client in order of the client's preference (favorite choice first). Each ciphersuite defines a key exchange algorithm (e.g. RSA), a bulk encryption algorithm (e.g. AES12) and a hash function (e.g. SHA1). The server will select a cipher suite or, if no acceptable choices are presented, return a handshake failure alert and close the connection10. As a consequence of the Handshake exchanges, each entity will generate the same session key (master_secret in the TLS terminology). Once the transport connection is authenticated and the session key is established, data exchanged by application protocols can be protected, applying the selected cryptographic methods and the sessions key. The TLS server authentication is usually by default, using a certificate and public key infrastructures (PKI). The client authentication method is determined during the Handshake phase and depends on the selected cipher suite. The server could be configured to explicitly authenticate the client at the TLS layer, or leave it to the application layer. In this latter case, only the server will be authenticated by TLS.

4.2. Certificate Structure

It is obvious that in practice it is very difficult to establish a confidential relationship between the various commercial certification authorities (CAs). We observe a closed system with respect to ISPs and their subscribers. The ISPs directly manage their own users account. In addition, a roaming agreement has to be established a priori by the participant ISPs in

order to provide roaming service. Thus we propose that the certificates should be issued by the ISPs themselves, not by the commercial CA. [7]. The idea is: a user (U), its home network (HN) and the network to visit (VN), the two networks share a priori a roaming agreement, in which each ISP has a roaming asymmetric key with pair (P_{KR}: public roaming key and S_{KR}: private roaming key). When the user wants to leave his home network he must obtain the public key P_{KR} that he will use in the authentication process in the visited network. In addition the network (VN) has its own private key S_{KV}, its corresponding certificate (which contains its public key P_{KV} and a signature on the same key with the private key of the HN network S_{KH}) and the public key of the HN network P_{KH}.

4.3. Proposed Authentication Scheme

Our scheme is as follows:

Step(1) Roaming user → Visited Network
$E_{P\,K\,R}$ (H, N_U, P_{KU})

Step(2) Visited Network → Roaming user
E_{PKU} ($Cert_V$, N_V)

Step (3) Roaming user → Visited Network
E_{PKV} (K, $Cert_U$), $Sign_{SKU}(N_U||N_V||V||U)$

Step(4) Roaming user ←→ Visited Network
E_K (exchanges)

4.4. Progress of the operation:

In the first step the user send the ID of its home network (H), its public key (P_{KU}) and a random number N_U used as nonce to the visited network encrypted by the roaming public key E_{PKR}.

In the second step if the visited network can decrypt the message with the roaming private key given exclusively to all operators having an agreement, the authentication procedure will continue, otherwise the procedure ends at this stage. If it comes to decrypt the message the visited networks (VN) take the sent ID and seek the correspondence certificate ($Cert_V$) signed by the corresponding network private key (S_{KH}). If find it the authentication procedure will continue, otherwise the network does not have a roaming agreement or agreement has expired with this network (HN). Therefore the user will be refused. Once the visited network has the public key of the user, it can encrypt with this key the response by sending the found certificate and a random number N_V used as nonce.

In the third step, the user can decrypt the message with its private key S_{KU} and thus can verify the validity of the certificate with the public key of his home network (P_{KH}). He will choose a random number (k) that will be used as a session master key and send this key with its certificate encrypted with the visited network public key. In addition the user signs the message (N_U ||N_V ||V ||U) using his private key S_{KU} where V and U are the identities of the visited network and the roaming user.

This signature serves as footprint that the user has used the service of this visited network and therefore this network may request a payment for this service for example.

5. PERFORMANCE ANALYSIS

We evaluate our proposal, taking into account the goals set in the design of the protocol on security needs in WATM. Our proposal satisfies the goal as follows:

- Our scheme has strengthened confidentiality in exchanges between the visited network and the user employing an asymmetric encryption with RSA 1024-bit encryption [8], with the introduction of a random number as nonce which ensures the freshness and prevent from reply attack using timestamp given the possibility of intercepting messages on the radio interface.
- The integrity of information is assured by the SHA-256 hash functions since the MD5 algorithm is beginning to be abandoned because of the found collisions [9], [10].
- The largest party and novelty in the proposed scheme is the introduction of the concept of non-repudiation in step 3 of our

scheme by adding a digital signature of the user with a standard algorithm such as the DSS [11], which was missing in the protocol SSL v3.0 and TLS v1.0.

- All these aspects of security are made to ensure a fast and efficient authentication service.

5.1. Security Feature Comparison

TABLE II summarizes a security feature comparison between the proposed protocol and previous proposals. Our protocol has the advantage over the work of D. Patiyoot et al. [6] of not using a third authority for authentication and it is much more practical and efficient in terms of communication and computation cost.

Table 2. Security Feature comparison.

	Delay (ms)	Number
RSA-1024 encryption	0,16	3
RSA-1024 decryption	5,00	3
AES-128 encryption	0,078 s*	1
RSA-1024 signature	4,95	1
RSA-1024 verification	0,16	1
DSA-1024 signature	2,79	1
DSA-1024 verification	3,21	1
SHA-256	0,011	2
SSL v3.0 Handshake	17	1

5.2. Experimental results

Our experimental work was done in two phases:

1) The time measurement of basic cryptographic functions such as RSA-1024 algorithm (encryption-decryption) for asymmetric parts, the hash function SHA-256, the AES-128 symmetric encryption algorithm for the final session key and both the RSA-1024 and DSA-1024 digital signature algorithm These measurements were made on a dual processor INTEL(R) Pentium(R) 4 machine with a clock speed of 2.80 GHz and a 512 Mb of memory using the crypto++ library [12].
2) Time measurement of the SSL v3.0/TLS v1.0 handshake protocol operation done on the mail server of our university with an INTEL(R) Pentium(R) 4, 3.20 GHz computer with 1024 Mb. of memory using the SSLdump software[13] for the measurement.

The calculation obtained for the SHA-256 hash operation is reached on a certificate of 900 byte and the AES-128 symmetric encryption calculation is made with a 4194304 bytes which yields a calculation time of 0.078 s with an average speed of 51.28 Mb/s.

According to the results, it is clear that our scheme of authentication is reliable since it does not depend on the home server especially if it is far or under a load or down. Lastly the time delay of authentication is less than one second as shown in TABLE III.

Table 3. Time measurement.

	D. Patiyoot et al.[6]	Proposed Protocol
The number of asymetric encry/decry	5	3
The number of digital signature	0	1
Time communication between Home and Visited networks	Yes	No
Impact Resulting from home network failure	Maximum	Maximum

6. CONCLUSION

In this paper we presented a new optimized scheme for fast authentication. Our scheme is based on the idea of building an independent authority between access providers resulting a reduction in terms of confidence as long as the certificates are issued by the ISP's themselves. In addition, our scheme uses SSL v3.0/TLS v1.0 enhanced security with asymmetric algorithms. The most significant function is the addition of a digital signature to the user for possible accounting. The proposed scheme in general is based on the idea of an independent authentication between the user and visited network without the direct intervention of the home network resulting in a huge gain in terms of time especially if the home network is remote or down. Remains to add a simulation work in the future to complement this work.

REFERENCES

1. G. Horn, B. Preneel, "Authentication and payment in Future Moble Systems.", *Computer Security-ESORICS'98, Lecture Notes in computer Science*, 1485, 1998, pp. 277-293.
2. C. Boyd, A. Mathuria, "Key establishment protocols for secure mobile communications: A Selective survey", *Information Security and Privacy*, *LNCS 1438, Springer-Verlag,* 1998, pp.344-355.
3. A. Adhav, T.S. Lee, S. Ghosh, "A modeling and simulation methodology for analyzing ATM network vulnerabilities", *ELSEVIER Science, Computer communications*, 2005, vol. 28, no11, pp. 1317-1336.
4. D. Raychaudhuri, "Wireless ATM networks: Technology status and Future Directions", *Proceedings of the IEEE*, Vol. 87, N. 10, Otober 1999.
5. S. Zhou, J. Chan, A. Seneviratne and T. Percival, "A Mobility-Enabled Hybrid Wireless Network with Standard ATM Backbone Switches: Architecture, Implementation and Performance," *Proc. IEEE WCNC99*, Sep.1999, pp. 388-392.
6. D. Patiyoot, S.J. Shepherd "Techniques for Authentication Protocols and Key distribution on Wireless ATM Networks", *Operating Systems Review*, Vol. 32, N. 4, 1998, pp. 25-32.
7. M. Long, C.-H. Wu, J.D. Irwin, "Localized authentication for wireless LAN inter-network roaming", *Proc. IEEE Wireless Communications and Networking Conference (WCNC), Atlanta, GA,* Mar. 2004, pp. 264-267.
8. R. Rivest, A. Shamir, L. Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM,* 1978, Vol. 21 (2), pp.120-126.
9. X. Wang, D. Feng, X. Lai, H. Yu, "Collisions for Hash Functions MD4, MD5, *HAVAL-128 and RIPEMD,*" CRYPTO 2004, http://eprint.iacr.org/2004/199.pdf.
10. P. Hawkes, M. Paddon, and G.G. Rose, "Musings on the Wang et al. MD5 Collision" *http://eprint.iacr.org/2004/264.pdf.*
11. *FIPS PUB* 186-2, "Digitale Signature Standard (DSS)," January 27, 2000.
12. Wei Dai, The crypto++ library, *http://www.cryptopp.com/.*
13. Rescorla, E, *http://www.rtfm.com/ssldump.*

Hadj GHARIB

Mathematics Laboratory
Djillali LIABES University
Sidi Bel Abbes, Algeria
Email: gharib@univ-sba.dz

Nidal ABOUDAGGA

Université Catholique de Louvain
UCL-Crypto group, Belgium
Email: aboudagg@dice.ucl.ac.be

Aoued BOUKELIF

RCAM Laboratory
Djillali LIABES University
Sidi Bel Abbes, Algeria
http://boukelif.wordpress.com/