IMAPS: Imbricated Authentication Protocol Suite for Mobile Users and Groups

Nidal Aboudagga*,Giacomo de Meulenaer*, Mohamed Eltoweissy† and Jean-Jacques Quisquater*
*UCL-Crypto group, Place du Levant 3, 1348 Louvain la Neuve, Belgium
Email:{quisquater, aboudagg, demeulenaer}@dice.ucl.ac.be
†Advanced Research Institute, 4300 Wilson Blvd., Suite 750, Arlington, VA 22203, USA
Email:toweissy@vt.edu

***Abstract*— The rapid advancement and the wide-spread use of the Internet and wireless communications in our professional endeavors and personal lives are making ubiquitous authenticated connectivity for mobile users indispensable. Individuals and groups may roam within a network or across networks, either in infrastructure or ad hoc mode. In any case, uninterrupted authenticated communication would be required for numerous applications, in particular real-time multimedia applications. In this paper, we propose an imbricated protocol suite for authentication in different mobility contexts at both the intra- and inter-network levels. To the best of our knowledge, this is the first comprehensive treatment of authentication in mobile networks. We demonstrate that our solution supports seamless secure mobility while incurring low overhead in the authentication process.**

I. Introduction

Over the past two decades wireless networks have become widely diversified ranging from cellular and satellite networks to wireless local area networks and ad hoc networks, constantly growing and providing mobile users with richer connectivity. Numerous types of wired and wireless networks are now converging in order to provide an ever-growing panel of ubiquitous services and products. Indeed, mobility is the most obvious advantage of wireless connectivity. The widespread deployment of wireless networks has increased dramatically the service demands and expectations of mobile clients, especially for real-time multimedia applications and communication. However, the limited coverage area of disparate networks, Base Stations (BSs) and Access Points (APs) makes inevitable the handoff between APs, BSs and networks while roaming. This process must be secure and fast enough to ensure continuous connectivity and collaborative operations among nodes and groups using different wireless technologies and administrative networks. Wireless networks, similar to other networks, must ensure the basic security functions confidentiality, integrity, non-repudiation and authentication for users and resources. This work focuses on authentication as the most fundamental security function.

The authentication of entities in wireless environments is a challenging proposition due to the vulnerability of the wireless medium to eavesdropping and the lack of centralization of wireless network organization. Wireless networks need to re-authenticate a node (or a group of nodes) each time that node (or group of nodes) changes the attachment point. Moreover, network visitors must also be authenticated when they do not share a previous security association with the visited network. Furthermore, in a peer-to-peer session, nodes may need to authenticate their peers, which can be in the same network or in foreign networks. In addition, these peers may need to re-authenticate each other for every new and recovered session.

Most of the existing authentication protocols provide efficient solutions for authentication either intra-network on inter-network, but not both. For example Mishra et al [1], Park et al [2] [3], and Aboudagga et al [4], enhance the efficiency of the authentication process only when mobility is predicted to be intra-network. On the other hand, protocols in [5] [6] [7] and [8] handle authentication for mobility across networks. Integration of such solutions to cover both intra- and inter-network authentication is non-trivial. Furthermore, mobile group authentication and authentication in a mixed mode (ad hoc and infrastructure) make such integration more challenging.

In this paper, we propose IMAPS, IMbricated Authentication Protocol Suite, as a comprehensive solution for authentication in mobile environments regardless of the mode of operation. Specifically, our protocol suite has the following features: (i) it provides intra-network as well as inter-network entities' authentication; (ii) it allows authentication in both ad hoc and infrastructure modes; and (iii) it provides both mobile group and mobile individual node authentication. The protocol suite also satisfies the following key requirements: (i) it does not require expensive additional infrastructure deployment; and (ii) it is efficient; i.e. supports seamless secure mobility while incurring low overhead in the authentication process. The latter requirement becomes crucial when wireless networks are used by mobile users for time sensitive applications like multimedia streaming and communication among mobile rescue personnel in disaster situations.

The remainder of the paper is organized as follows. Section II provides an overview of the basic constructs of IMAPS. Section III details IMAPS functionality and its management architecture. Section IV presents security and performance analysis. Related works are presented in section V. Finally, the paper concludes in section VI highlighting future work.

II. IMAPS Constructs

This section describes the basic constructs of IMAPS while the next section details its construction. IMAPS employs

and extends the authentication methodology we developed in [9] (generic authentication process), [8] (group authentication protocol, mGAP) and [4](inter-network authentication ticketing protocol). We also use a cryptographic primitive that is described in [10]

Authentication model: the proposed imbricated protocol suite provides authentication following the generic authentication model we developed in [9]. This model comprises several generic steps: bootstrapping, pre-authentication, credential establishment, authentication, and finally expiration or revocation of credentials. An authenticating node can go back to credential establishment using credential renewing. Generally, authentication protocols follow these steps, albeit, to varying degrees.

Mobility profile: mobility prediction is a primordial component of the imbricated protocol suite. It enables us to provide a mobile entity (node or group of nodes) with authentication credentials for a large set of networks before the entity leaves the home network. Mobility prediction is based on entity profiling (details are in

Authentication credentials: IMAPS is based on providing the mobile entity (node or group of nodes) with a mobile credential tailored to the mobility profile of each entity. The credential is based on our group authentication protocol mGAP [8] and a cryptographic primitive described in [10], which allows any one of n group members to select t members from n to whom it targets a message in such a way that only one of t is sufficient to decrypt the message.

Thus after the initial authentication by the visited network, it creates then distributes authentication credentials to the predicted internal roaming destinations according to its internal mobility prediction scheme. The distribution and the creation of these credentials use the concepts of our authentication ticketing scheme in [4]. Therefore, the visitor entity and the visited network use the master secret resulting from the first authentication to derive the roaming credentials. Moreover, when the roaming destinations receive the authentication credential of the roaming entity, they cannot only authenticate the roaming entity, but also renew independently the authentication credential for recurrent visits.

III. Imbricated Authentication Protocol Suite

The imbricated protocol suite considers the mobile entity either as a support for a mobile group or as an individual mobile node. In the home network, the mobile entity can be either a member of an ad hoc network or an access point offering access to a set of mobile nodes. In both cases, the mobile entity uses the imbricated protocol suite to authenticate itself or to authenticate on behalf of its attached nodes. After the profiling process at the home network, the mobile node is provided with the adequate roaming credential for a list of networks in its profile.

The roaming credential design is based on the cryptographic primitive described in [10], which allows any member of targeted t member subset of an ad hoc group of n receivers to recover the message. The notation of this scheme is $(1, t, n)$ where 1 means that one receiver decrypts the message, 't' represents the number of targeted members from n, and n is the total number of group members formed by the sender(home domain HD). For the protocol notations see table I

TABLE I
THE PROTOCOL NOTATION.

U,HD,V	mobile entity, home domain, visited domain identities
SUB	subscription contract includes: validity time, authorized services, (U), (HD), S_U
S_U, s_U	mobile entity verification and signature public key pair
S_{HD} and s_{HD}	home domain signature/verification public keys pair
N_A, N_U,N_V	user nonce's, visited domain nonce's
K_{HD-U}	shared key between HD and mobile entity
K	roaming authentication key delivered by HD
H	a hash function
$PKG(1,t,n)$	public key to encrypt messages group of domains t from n
Ticket	$E_{PKG}\big(K, SUB, s_{HD}(K, SUB)\big)$
The authenticator	$E_K(SUB, N_U, N_V)$
$E_V(N_U, N'_U)$	Encryption of the nonces with the public key of V
MK	A master key resulting from across network authentication
PMK_i	pairwise master key shared for authentication with AP_i
Crd_i	(ID_{AP_i},$E_{K_i}(PMK_i$, ID_U,Times))
K_i	secret key shared between the server of the visited domain and APs in visitor mobility pattern
n	number of roaming destination in the mobility pattern

Differently from mGAP, the execution of IMAPS results in a pairwise secret between the visited network and the mobile entity. Moreover, IMAPS proactively creates and distributes the authentication credentials for roaming within the visited network. These credentials are based on modified functions of our authentication ticketing scheme [4]. The protocol exchanges are processed as follow.

1) $U \longrightarrow HD : U, N_A$
2) $HD \longrightarrow U : Ticket, E_{K_{HD-U}}\big(K, N_A, SUB\big)$
3) $V \longrightarrow U : N_V$, $Cert(V)$
4) $U \longrightarrow V : Ticket, Authenticator, E_V(N_U, N'_U)$, $s_U(H^n(N_V, N'_U), V)$
5) $V \longrightarrow$U: $E_K(N_U, N'_V)$
6) $V \longrightarrow AP_0$: Crd_i, $0 \leq i \leq n$
7) $AP_0 \longrightarrow AP_i$: Crd_i, $0 < i \leq n$

We now describe the steps of IMAPS according to the authentication model in section 2.

• *Bootstrapping:* the home network provides the mobile entity with a shared symmetric secret (K_{HD-U}), a contract that contains the mobile entity's public key certificate, validity time, authorized services, the identity of the mobile entity and the identity of the home network. The home network also provides the mobile node with a ticket, namely, the roaming

authentication credential according to its mobility profile. The mobile node as well as the authentication servers of the potential visited networks are bootstrapped with equation (1). This is used for the proactive derivation of the authentication credential for roaming within the visited network.

$$PMK_i = TLS\_PRF(MK, H(MK \| U\_MAC \| AP_i\_MAC)) \quad (1)$$

The pairwise key PMK_i is the master key distributed by the authentication server of the visited network proactively to the next potential roaming destination AP_i of the mobile node U. MK being a master secret resulting from the across network authentication with the imbricated protocol suite. AP_i_MAC and U_MAC being respectively the access point and the mobile node MAC addresses, i is the index of the AP $(0 \leq i \leq n)$, where n is the number of APs in the mobility pattern of the visited network and H is a secure one way hash function.

The APs, as well as the servers of the visited network, are bootstrapped with the mobility patterns and a shared key k_i between the server and each AP. Finally, they are bootstrapped with equation (2) for the computation of the credential for recurrent visits.

$$PMK_{im} = TLS\_PRF(H^m(PMK_i), Counter \| STA\_MAC \| AP_i\_MAC) \quad (2)$$

Where PMK_{im} is the pairwise master key proactively derived by the AP_i and mobile node U for authentication at the m^{th} visit.

• *Pre-authentication:* Starts when the mobile node U arrives at the visited domain V, and receives from the latter the nonce N_V and the certificate $Cert(V)$ in message (3). Consequently U generates two nonces N_U and N'_U. U creates the authenticator using K . U uses the visited network public key to encrypt both nonce N_U and N'_U for V. U also computes the signature $s_U(H^n(N_V, N'_U), V)$. Finally (U) sends the previous values as well as the ticket received in message (2) to the visited network. The pre-authentication step finishes when the visited domain V receives message (4).

• *Credential establishment:* Starts when the visited domain V handles message (4), since it decrypts the ticket, recovers K, decrypts the authenticator, recovers N_U, N_V and SUB. V also verifies that the N_V matches the one it was sent in message(2), then establishes K as authentication key. V decrypts $E_V(N_U, N'_U)$. V creates a new nonce N'_V and computes the master secret $MK = H(N'_U, N'_V)$ between V and U. This completes the credential establishment and the one-way authentication U to V.

The authentication server of the visited network computes, according to its roaming pattern, a set of authentication credentials using equation (1) for local roaming. This completes the credential establishment and the one-way authentication U to V. The session key between the primary AP and the mobile node will be derived from the PMK_0.

• *Authentication:* When the mobile node (U) receives message (5), it knows that it is authenticated to V and can authenticate V. Message (5) confirms to U the authentication key K. This also means that the mobile node is pre-authenticated to the APs in the mobility pattern, since the primary AP has already received roaming credentials in message (6) and distributes these local authentication credentials to those APs ahead of the mobile node motion in message (7). Thus, the mobile node and the primary AP can start a challenge/response based on a four-way handshake [11] session key derivation using PMK_0.

For recurrent visits the APs compute and cache an authentication key for the next expected visit of the mobile node after the latter leaves. Equation (2) shows how the authentication material of recurrent visits is computed.

• *Monitor behavior:* The visited domain V monitors the validity of the mobile node credentials and subscription contract SUB. If the credentials and the contract are expiring, a new authentication process is started from the credential establishment step. On the other hand, the authentication material for intra-network authentication are created with validity duration matching the contract condition and validity. However, if the roaming agreement between home network and visited network allows contract renewing at the visited domain, the credentials can be created extending beyond the initial contract date limits. The storage duration of pre-authentication credentials and recurrent visits authentication is set according to the visited domain policy.

IV. IMAPS Analysis

(In this section we report on the security and performance aspects of IMAPS.

A. Security analysis

We consider a threat model where an attacker can be active or passive, thus he can attempt to eavesdrop on exchanges, inject messages, alter the exchanges, or replay old messages. We assume that each network authority has or can easily obtain the authentic public key of the different network authorities. Since there are roaming agreements, each network authority's public key is certified by the other networks' authorities party to the roaming agreement. This is a reasonable assumption since the number of networks is much smaller than the number of mobile entities. Given this threat model and the above assumptions, the reaction of IMAPS can be summarized as follows:

• The protocol provides the mobile node with a fresh roaming authentication key 'K' via a secure message (encrypted using the long term shared key K_{HD-U}) in message (2). An attacker can neither recover K without knowing K_{HD-U}, nor can he use an old key since the roaming authentication key K is encrypted and sent with the nonce N_A received by HD in message (1). The presence of N_A in the non-ticket part of message (2) proves the freshness of K for the mobile entity U.

• Message (2) also includes a ticket, which is the transportable credentials, needed to authenticate the mobile node to the visited network and vice versa. This ticket is encrypted using the entity's public key encryption algorithm. The ticket also includes K and SUB as well as their signature by HD;

therefore an attacker (non member) of the group cannot recover K.

• The signature of HD over (K, SUB) provides V with an authenticated key. The signature of HD ensures the non-repudiation of roaming credential by HD to V; moreover, the signature of the SUB by HD certifies the validity time, the allowed services, the roaming entity identity, and Us signature verification key.

• Message (3) of the visited network to the mobile node, provides the latter with a certified public key of the visited network that is easy to verify since it is assigned by the home network of the mobile node. Message (3) also contains a nonce that will be used by the mobile node in message (4) to prove the freshness of the latter.

• Once message (4) is received, V decrypts the ticket to recover K and decrypts the authenticator. Only a member of the group can decrypt the ticket and the authenticator. The presence of N_V sent to U in message (3) within the authenticator, proves the freshness of the authenticator and proves that U knows the key K, therefore an attacker can not impersonate U to V, or even replay an old authenticator.

• The signature part in message (4) again proves the identity of U and that U asks the access to the nominated domain in the signature. An attacker can not impersonate U to create a fresh signature. The signature also contains N'_U which provides V with authentic contribution in the master key creation. The value $E_V(N_U, N'_U)$ provides V with N'_U in a secure way, because only V can recover N'_U since it is the only one possessing the private key to decrypt $E_V(N_U, N'_U)$.

• The freshness of the signature is ensured by the presence of N_V. The fresh signature of U includes the identity of the chosen domains. This shows from which domain the service was requested and allows for protection against impersonation and rogue domain. However, the domains of the profile, that have not been chosen for the present transaction, are trusted to not impersonate each other to the mobile entity. The n^{th} hash included in the signature allows the mobile entity to request different services or different parts of services. This is implemented by giving an earlier signed hash value from the given hash chain instead of re-authentication. This practice is often used in micro-payment schemes [12].

• When V processes the different part of message (4) it creates the nonce N'_V. So that it can compute the pairwise master keys (PMK_i) for the primary access point AP_0 and the APs in the local mobility pattern. The keys PMK_i will be the re-authentication basis within the network for the mobile node. Moreover the PMK_i will be the basis of session key derivation between the mobile node and the APs in the local mobility pattern. Thus, the transaction inside the visited network will be secure even against the other networks in the profile of the mobile node.

• When the mobile node receives message (5) the mutual authentication across networks is accomplished. This message contains the visited domain contribution N'_V in the creation of the master secret MK. Thus, the mobile node can compute PMK_i for authentication while roaming within the network.

• For future across network roaming, V and U repeat exchanges (1) and (2), where V will use a new nonce $N_A^{'}$ and will create a new ticket. V also uses the session key previously derived from PMK_is to provide U with a new authentication roaming key $K\prime$. Note that tK, the session key as well as K_{HD-U} are at least AES-128 keys, used for limited time and specific operations. Their corruption by an attacker is impossible in practice.

B. Performance Analysis

IMAPS supports authentication of roaming entities across networks in both infrastructure and ad hoc modes. Moreover, it supports the authentication of mobile entity accompanied by a group of mobile nodes and authenticating on behalf of them.

• IMAPS does not require a high amount of storage or pre-computation from the mobile node before roaming to a new destination. The MN can update its profile, and it is not obliged to select in advance its roaming destination. IMAPS shifts most of the computational burden on the domain side, and uses low cost primitives [13].

• The storage space requested in the IMPAS at the mobile node side for the ticket is reasonable and less then 2Kbits, while the PMK_i are recomputed instead to be stored. From the communications perspective, IMAPS uses only three message exchanges (messages 3, 4 and 5) to perform a mutual authentications and key establishments between U and V.

C. Sample Implementation of IMAPS

Our strategy is to test IMAPS's implementation in a resource-constrained network. We report on the communication overhead of IMPAS in such a restricted environment. We implement IMAPS on Micaz nodes (with 8-bit microcontroller Atmega 128L). The network uses the frequency 2.4 GHz and it is IEEE 802.15.4 compliant. The platform provides for up to 250 kbps data rate.

1) Experiments:: In the experiments conducted, we have run IMAPS between the mobile node U and the node V in the visited network. the node V is networked with V_a, V_b, V_c and V_d in ad hoc mode. Node V can also be either directly connected to a distant node HD from U's home network or via intermediary relay, R_1, $R_1 \ldots R_n$. to perform proxy authentication of U. Moreover, after U is authenticated by V, it can roam to any node of the group V_a, V_b, V_c, V_d using IMAPS. In our experiments, the visitor U authenticates to V using IMAPS. U performs this authentication when V is under different computation load. This for first authentication, then, U authenticate to one of the nodes networked with V, such as the group V_a, V_b, V_c and V_d, using the feature of intra-network authentication IMAPS (see figure 1). Intra-network authentication is also performed for different loads. The load on the authenticator node is specified as the time after which the node is able to process a new coming request.Thus we can measure the latency of the authentication process to compare the performance of different authentication alternatives. For the proxy authentication,in addition to varying the load on HD, we have varied the number of intermediary relays between V and HD.

As we are interested in performance based on latency variation, for simplicity, the latency of cryptographic operation

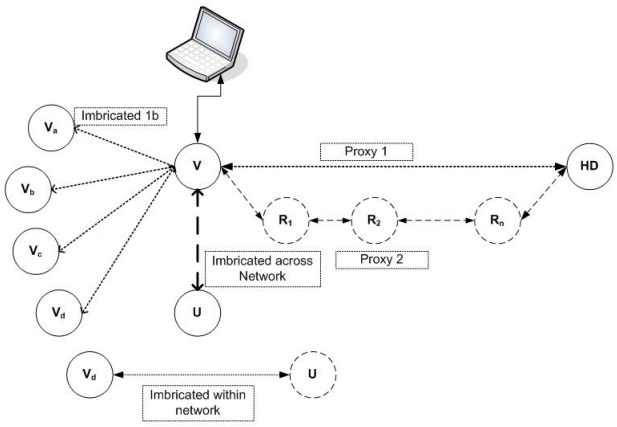

Fig. 1. Network Model

was replaced in our implementation by a dummy one. The used values were from work on optimized implementation of cryptographic operation in sensor networks [14], [15]. The used values are for 160-bit elliptic curve digital signature algorithm ECDSA sign:1.925s 160-bit elliptic curve digital signature algorithm ECDSA verify: 2.433s, 128-bit AES encrypt/decrypt for 16 bytes: 3.75 ms, AES is also used to compute hash values/

The table below presents the authentication latency when using different authentication protocols on the Micaz nodes. These values are computed without any load on V or on

TABLE II
THE PROTOCOL LATENCIES.

Protocol	Latency
Imbricated across networks	6448 ms
Imbricated within network	115 ms
symmetric proxy	122 ms
asymmetric proxy	6795 ms
EAP-TLS	8800 ms

HD. IMAPS is executed between U and V. while the inter-network authentication using IMAPS is reduced to a session key derivation; as described by the four way handshakes protocol of the security standard IEEE 802.11i. This because the authentication credential was distributed ahead of the mobile node U to V_a, V_b, V_c and V_d. However by proxy symmetric authentication protocol transfers the request of U to the home demain HD of the latter (i.e. GSM network). While the proxy asymmetric protocol performs the authentication of mobile node in the same way but uses asymmetric cryptography.

2) Results: When there is no load on the network, the protocols have the nominal latencies shown in table 2. As the imbricated protocol suite for across and within network authentication is always faster than proxy asymmetric protocols. We do not analyze the proxy asymmetric authentication protocol any further.

The authentication latency of a symmetric mutual authentication protocol depends on the number of the intermediary relays in the path between V and HD. We notice from our implementation that each relay adds approximatively 16,75 ms, if we consider no specific load on the relays of the path V to HD. Figure 2 shows the latency of the different protocols when there is equal load on V and HD and no relays between them. The result shows a net advantage for proxy authentication but this process must be repeated each re-authentication. However, with imbricated protocol only the first authentication is costly while the re-authentications for roaming in the same network will use the generated credential for within network authentication. Hence the imbricated protocol became faster then proxy authentication. Moreover, the network condition can change at any moment and the proxy authentication can fail or slow down. Furthermore, in real conditions, often the proxy authentication passes through several relays incurring many encryption/decryption and path related delays.

Figure 2 shows the latency impacts of an increasing load applied the both V and HD. We can see that the latency of imbricated protocol for across network authentication is higher than the latency of symmetric proxy authentication, but the authentication latency of the imbricated protocol for within network roaming continue the be lower than the proxy protocol.

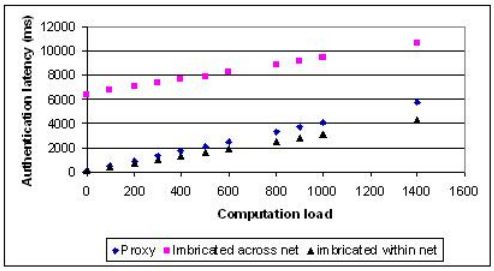

Fig. 2. Latency variation of imbricated protocol for within and across network authentication VS symmetric proxy authentication. The same load is applied on V and HD and no relay between V and HD

When the proxy authentication request have to cross several relays in the path between V and HD, the authentication latency increases aromatically. It covers the communication latency introduced by each relays and the latency due to the computation load on V,on the relays R_i, and on HD. However , the latency introduced by the relays R_i and HD does not impact the imbricated protocol, because the latter treats locally both across and within network authentication .

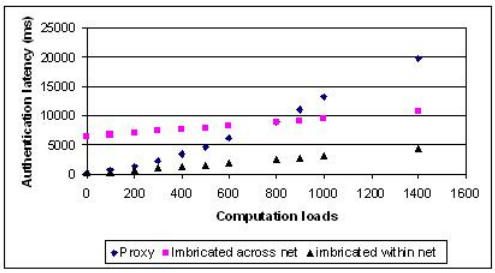

Fig. 3. Latency variation with increasing number of relay between V and HD and increasing load on the relay .

From figure 3 we can conclude that first authentication with imbricated protocol become faster than proxy authentication

starting from the point where there is 7 relays with moderated load are in the path V to HD. This shows clearly the advantage of the imbricated protocol that against the symmetric proxy authentication in real network conditions.

The consideration of other kinds of network should modify these results in favor of IMAPS. Wireless Sensor Networks (WSN) are indeed not suitable for heavy public key cryptography (PKC) computations as opposed to i.e WLANs. In WLANs, PKC computations can be 700 times faster than in WSN (see [16], with an AMD Athlon 1467 MHz) while communications have a throughput roughly 150 times bigger (practical throughput of 19 Mbps in 802.11g). A quick estimation for a WLAN in a similar situation as described before (loads scaled down by 700) gives the following latencies: 8 ms for across network authentication with imbricated protocol , 2 ms for within network. However proxy symmetric authentication costs 3.3 ms. Consequently, the number of relays from what imbricated protocol become faster than proxy scheme is lowered to the value of 4. This is because the latency of imbricated protocol is mainly composed of computations delay, while the latency sources of the proxy symmetric protocol more diversified. Further simulations are needed to provide more accurate results.

V. Related work

To the best of our knowledge, our work is the first to present a comprehensive solution adaptable to both intra-network and inter-network authentication. In cellular networks, the mobile node (MN) and the authentication center (AUC) use shared key and a challenge response scheme for authentication [17], [18], [19]. When roaming, the MN is authenticated by proxy to its old location. The ITF developed the mobile Internet protocol (MIP) for security and mobility management across networks. Unfortunately, the MIP induce latency due to the heavy computation [5], [20] and multi proxy operation [6], [21]. Recently, MIP authentication was enhanced to reduce latency using broker entities at the networks edges [7], [12].

Other architectures use expensive key agreement protocols [22], [23], where the parties contribute in authentic session key establishment for each session and new coming node.

Other works have focused on reducing the authentication latency for a roaming node within the same network via proactive [11], [2], [3], [1] or reactive [11],[1] authentication of the MN, and also via hybrid hybrid way [4]

VI. Conclusion

This work presented IMAPS, an imbricated authentication protocol suite for authentication in different mobility contexts and for different wireless network modes. Our alchemy combine credential transportability with proactive credential distribution, and profiling with network specific roaming prediction scheme. We demonstrated the advantages of using our profiling scheme to create unique transportable credentials for across networks authentication. Moreover IMAPS supports more freedom of roaming of mobile entities within the visited networks. This is achieved without incurring resource-consuming operations or additional physical network infrastructure. IMAPS presents a clear enhancement of authentication performance as shown by the implementations results.

References

[1] A. Mishra, M. Shin, T. Clancy, and W. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 26–36, 2004.

[2] Y. C. Sangheon Pack, "Fast inter-ap handoff using predictive-authentication scheme in a public wireless lan," in *Networks*, ICWLHN and ICN. world scientific publisher, August 2002, pp. 15–26.

[3] ——, "Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model," in *Mobile and Wireless Communications*. Kluwer, B.V., 2002, pp. 175–182.

[4] J.-J. Q. Nidal Aboudagga, Mohamed eltoweissy, "Fast Roaming Authentication in Wireless LANs," in *2nd International Computer Engineering Conference: Engineering the Information Society, ICENCO 2006*, Cairo, Egypt, December 2006.

[5] C. Perkins and P. Calhoun, "Mobile IPv4 challenge/response extensions," IETF, november 2000, rFC 3012 (request for comments).

[6] S. Farrell, J. Vollbrecht, P. Calhoun, L. Gommans, "AAA Authorization Application Framework," IETF, August 2000, rFC 2904 (request for comments).

[7] M. Cappiello, A. Floris, L. Veltri, "Mobility Amongst Heterogeneous Networks with AAA Support," in *IEEE International Conference on Communications*, vol. 4. ICC, May 2002, pp. 2064–2069.

[8] N. Aboudagga, J.-J. Quisquater, and M. Eltoweissy, "Group authentication protocol for mobile networks," *wimob*, vol. 0, p. 28, 2007.

[9] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. DaSilva, and J.-J. Quisquater, "Authentication protocols for ad hoc networks: taxonomy and research issues," in *Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*. New York, NY, USA: ACM, 2005, pp. 96–104.

[10] V. K. W. J. K. Liu and D. S. Wong, "Custodian-hiding verifiable encryption," in *the 5th International Workshop on Information Security Applications*, LNCS. Springer-Verlag, October 2004, pp. 51–64.

[11] "Ieee std 802.11i-2004 ieee standard for information technology-telecommunications and requirements part 11: Wireless lan medium access control (mac) and physical layer (phy)specifications amendment 6: Medium access control (mac) security enhancements," 2004.

[12] W. W. W. Liang, "A local authentication control scheme for efficient authentication in wireless networks," in *Proc. of 60th IEEE Vehicular Technology Conference, VTC 2004-Fall*, vol. 7. IEEE press, 2004, pp. 5276–5280.

[13] A. M. D. Johnsonm and S. Vanstone, "The elliptic curve digital signature algorithm ECDSA," in *International Journal of Information Security*. Springer Berlin/Heidelberg, August 2001, pp. 36–63.

[14] An Liu and Peng Ning, "TinyECC: Elliptic Curve Cryptography for Sensor Networks," Cyber Defense Laboratory, 2006, http://discovery.csc.ncsu.edu/software/TinyECC, September 2006.

[15] A. Vitaletti and G. Palombizio, "Rijndael for sensor networks: Is speed the main issue?" *Electr. Notes Theor. Comput. Sci.*, vol. 171, no. 1, pp. 71–81, 2007.

[16] B. Preneel and A. B. et al, "Nessie d17 - preliminary list of realistic performance estimates." [Online]. Available: citeseer.ist.psu.edu/article/preneel02nessie.html

[17] S. M. Redl, M. K. Weber, M. W. Oliphant, "An Introduction to GSM," Artech House, Tech. Rep., 1995.

[18] R. Kalden, I. Meirick, M. Meyer, "Wireless Interned Access Based on GPRS," in *IEEE Personal Communication*, vol. 7, April 2000, pp. 8–18.

[19] 3rd Generation Partnership Project3G TS 33.12, "Technical specification group services and system aspects, 3g security," 3GPP suport, http://www.3gpp.org/ftp/tsg_sa/WG3_Security/_Specs/33120-300.pdf, Tech. Rep. 5, 1995.

[20] S. Jacobs, "Mobile IP public key based authentication," March 1999, internet draft, URL:Draft-jacobs-mobileip-pki-auth-02.txt.

[21] M. Barton, D. Atkins, J. Lee, S. Narain, D. Ritcherson, K. Tepe, K. Wong, "Integration of IP Mobility and Security for Secure Wireless Communications," in *IEEE International Conference on Communications*. ICC, April 2002, pp. 1045–1049.

[22] A. E. E. Bresson, O. Chevassut and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices," in *Proc. of MWCN '03*, IFIP. World Scientic Publishing, October 2003, pp. 59–62.

[23] C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishement*. Springer, June 2003, pp. 190–195.