The Design of Efficient Internetwork Authentication for Ubiquitous Wireless Communications

Minho Shin, Justin Ma, William A. Arbaugh

{mhshin, jtm, waa}@cs.umd.edu
Department of Computer Science
University of Maryland
College Park, Maryland 20742, USA

***Abstract*— A variety of wireless technologies have been standardized and commercialized, but no single solution is considered the best to satisfy all communication needs due to different coverage and bandwidth limitations. Therefore, internetworking between heterogeneous wireless networks is extremely important for ubiquitous and high performance wireless communications. The security problem is one of the major challenges in internetworking. To date, most research on internetwork authentication has focused on *centralized authentication* approaches, where the home network participates in each authentication process. For high latency between the home and visiting networks, such approaches tend to be inefficient. In this paper, we describe *chained authentication*, which requires collaboration between adjacent networks without involvement of the home network. After categorizing chained protocols, we propose a novel design of chained authentication methods under 3G-WLAN internetworking. The experiments show that *proactive context transfer* and *ticket forwarding* reduce the 3G authentication latency to 36.8% and WLAN EAP-TLS latency to 23.1% when RTT between visiting and home networks is 200 ms.**

***Index Terms*— System design, Experimentation with Testbed**

I. Introduction

Wireless communication technology spans from Wireless Personal Area Networks (WPAN), such as bluetooth [1], to 3G Wireless Wide Area Networks, such as CDMA2000 and UMTS. Despite the variety of wireless technologies, no single solution is considered the best to satisfy all communication needs because of different coverage and bandwidth limitations. For example, 3G networks provide widespread coverage with limited bandwidth, up to 2 Mbps. However, WLAN provides high bandwidth, up to 54 Mbps, with relatively smaller coverage. For ubiquitous and high performance wireless networking services, the internetworking between wireless networks is extremely important. Most internetworking studies have been dedicated to the integration of 3G and WLAN (see [2], [3], [4], [5], [6], and [7]).

Security is one of the major challenges in internetworking. When the mobile station (MS) switches the connectivity to a different network, due to mobility or bandwidth demand, the mobile station and the network have to authenticate each other for secure communications[1]. However, the authentication process required by each network tends to be complicated and costly. For example, the GSM technical specification on performance requirements [8] assumes that the MS responds to an authentication request from the network in just under 1 second. In 802.11, EAP-TLS authentication takes about 800 ms [9]. Long authentication delays can cause a disruption of service that is noticeable to users.

Most research on internetwork authentication assumes that the visiting network should collaborate with the home network [6] [10] [11] [12] [13] [14], called *centralized methods*. In centralized methods, exchanging messages between the visiting network and the home network is inevitable for each authentication process. Fig. 1 illustrates a typical sequence of messages in centralized methods. Due to high latency between visiting and home networks, the authentication latency in visiting networks tends to be unacceptably high.

This paper describes a novel approach for designing fast internetwork authentication, called *chained authentication methods*. Unlike centralized methods, chained authentication is a distributed method in which authentication at a new network relies on the authentication at a previous network. Thus, chained methods do not require message exchanges with the home network (Fig. 2).

[1]Without loss of generality, we assume one network is controlled by one authentication server. Therefore, network refers to a domain or realm.

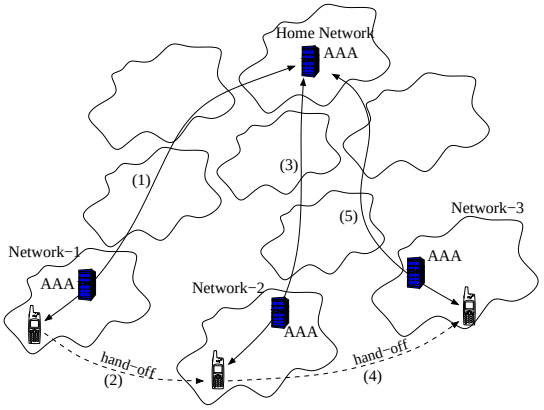

Fig. 1. *Centralized Method for Internetwork Authentication*

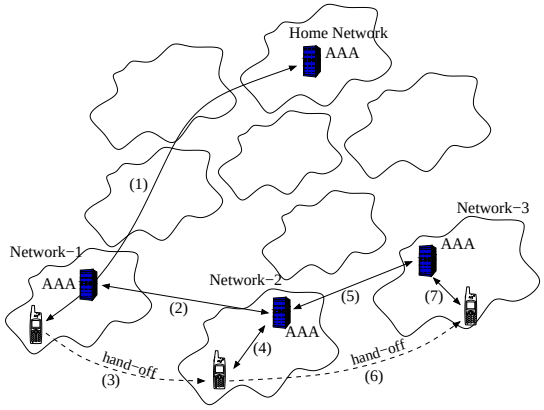

Fig. 2. *Chained Method for Internetwork Authentication*

Assume $\{N_1, N_2, \ldots, N_m\}$ is a network level mobility path, where N_1 is the home network (or the client is authenticated to N_1 through the home server). In chained authentication methods, the results of the authentication process in network N_i, such as credentials, become part of the input to the authentication process in network N_{i+1}. We categorize the chained authentication methods into *proactive context transfer*, *reactive context transfer*, and *ticket forwarding*. Fig. 2 shows the mobility path under proactive context transfer. To enable proactive context transfer, we propose a soft-prediction system by extending neighbor graph for the internetwork environment [15] [16]. The main advantage of the chained authentication approach is performance because authentication requires message deliveries no farther than the adjacent networks.

The contributions of our work are (i) a proposal for chained authentication methods as a fast and secure internetwork authentication framework, (ii) a categorization of chained authentication methods, and (iii) novel designs of each chained method category under 3G-WLAN internetworking, as well as a comparison of their performance by experiment.

We organize the rest of the paper as follows: We give background on wireless authentication methods in section II, and describe the chained authentication framework in section III. We propose novel designs for chained methods under 3G and WLAN internetworking in section IV, and present experimental results for these designs in section V. Section VI describes a soft-prediction scheme to assist the chained methods. Section VII describes related work, and we conclude in section VIII.

II. Background

In this section, we provide a brief review of the authentication protocols in 3G and IEEE 802.11. The two major 3G systems, UMTS and CDMA2000, adopted the same authentication protocol, AKA (Authentication and Key Agreement) [2]. Thus, we present AKA as the representative authentication protocol for 3G systems. For the authentication in 802.11 network, we assume that the network follows 802.11i RSN (Robust Secure Network) standard.

A. 3G Authentication - AKA

The AKA protocol was developed by fixing and expanding GSM's authentication method. AKA provides mutual authentication between the mobile station and the network. It also distributes cryptographic keys from the network to the mobile station.

The AKA procedure have two stages (Fig. 3). In the first stage, HLR/AC (Home Location Register/Authentication Center) transfers security credentials (in an authentication vector, AV) to VLR (Visitor Location Register) for voice traffic, or to PDSN (Packet Data Serving Node) for packet-switched traffic. The distribution of AV's should be protected by IPsec or an equivalently strong mechanism. An AV consists of RAND, XRES, CK, IK, AUTN, and optional UAK. HLR first generates RAND and derives XRES, CK, IK, and AUTN using the master key K as follows,

$$\begin{aligned} XRES &= f2(K, RAND) \\ CK &= f3(K, RAND) \\ IK &= f4(K, RAND) \\ AUTN &= SQN \oplus AK || AMF || MAC \\ MAC &= f1(K, SQN || RAND || AMF) \\ AK &= f5(K, RAND) \\ UAK &= f11(K). \end{aligned}$$

[2]CDMA2000 uses a slightly modified AKA which includes additional credential, UAK, to protect bogus shell problem [17].

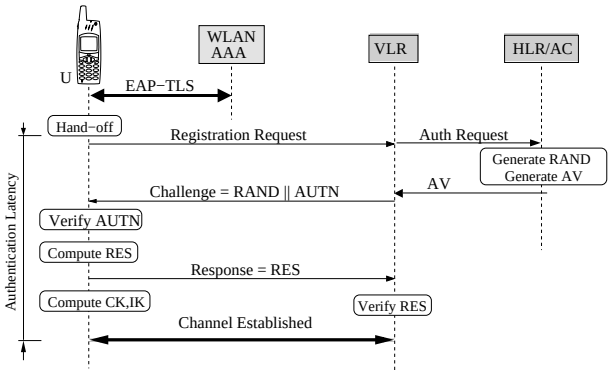

Fig. 3. *AKA: Authentication in 3G (UMTS and CDMA2000)*

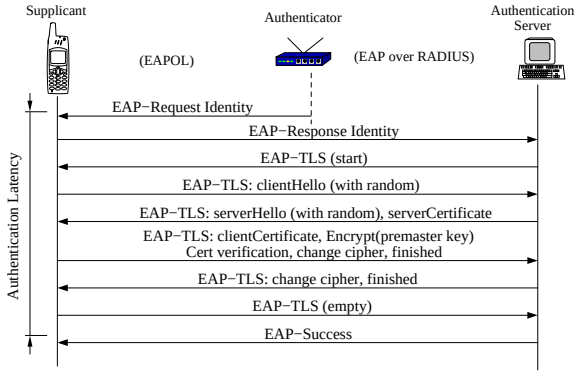

Fig. 4. *EAP-TLS message diagram*

where $f1, \ldots, f5$, and $f11$ are hash functions defined in the standard [18].

In the derivation of AUTN, the HLR uses a sequence number SQN to protect against replay attacks, and AK (Anonymity Key) is xor-ed with SQN to avoid identity tracking by observing SQN. AMF is an information field.

In the second stage, MS and VLR authenticate each other through challenge-response exchanges. First, the MS retrieves SQN from AUTN message as follows,

$$SQN \quad = \quad SQN \oplus AK \oplus f5(K, RAND).$$

Then MS checks if SQN is in a valid range. If this check fails, MS initiates a re-synchronization process. If SQN is valid, then MS authenticates the network by checking the MAC field of AUTN as

$$MAC \quad == \quad f1(K, SQN||RAND||AMF).$$

Once verified, MS calculates and sends RES to VLR.

$$RES \quad = \quad f4(K, RAND)$$

Now, VLR can verify if MS has the correct master key K by simply comparing RES with XRES from AV. Once verified, VLR uses CK and IK in AV for the secure channel. Meanwhile, with RAND from HLR and K, MS can calculate CK and IK, thus establishing the secure wireless channel.

B. WLAN Authentication - EAP-TLS

WEP (Wired Equivalent Privacy), the suggested security feature in the original IEEE Standard 802.11, is insecure [19] [20]. To amend this situation, IEEE standard work group 802.11i [21] has been working on a new security solution for 802.11 WLAN, called RSN (Robust Security Network). In RSN authentication, there are three entities: supplicant, authenticator and authentication server (AS). The supplicant is the user system that wants to access the network, such as a mobile station. The AS is the entity that authenticates the supplicant. RADIUS [22] server is a de facto standard for AS's. The authenticator facilitates authentication between supplicant and AS. In this paper, we assume that the authenticator is in the access points (AP).

RSN relies on IEEE standard 802.1x, a port based network access control. In 802.1x, any packet from the supplicant is not allowed to the network, except EAP packets, until the authentication procedure ends with success. 802.1x uses IETF EAP (Extensible Authentication Protocol [23]), originally designed for PPP dial-up connections. Over EAP, any challenge-response upper-layer authentication method can be used, such as TLS [24], Kerberos [25], LEAP (Lightweight-EAP) or PEAP (Protected-EAP). In this paper, we choose TLS over EAP (or EAP-TLS [26]) as the representative 802.11 authentication scheme. EAP-TLS is already commonly implemented for WLAN. Also, TLS is resilient to man-in-the-middle attacks and supports explicit mutual authentication using certificates from the supplicant and AS.

Fig. 4 shows the typical message flow of a successful EAP-TLS authentication. The supplicant and server exchange their random numbers and certificates. They authenticate each other by certificates and generate a 48 byte master key, MK. From MK, the client and the server generate session keys as follows,

$$SK \quad = \quad PRF_{128}(MK, \text{"client EAP encryption"}, clientHello.random||serverHello.random)$$

The first half of SK is used for encryption and the second half is used for message authentication key.

III. The Chained Authentication for Internetworking

Based on hop-by-hop trust associations between visiting networks, chained authentication provides a general

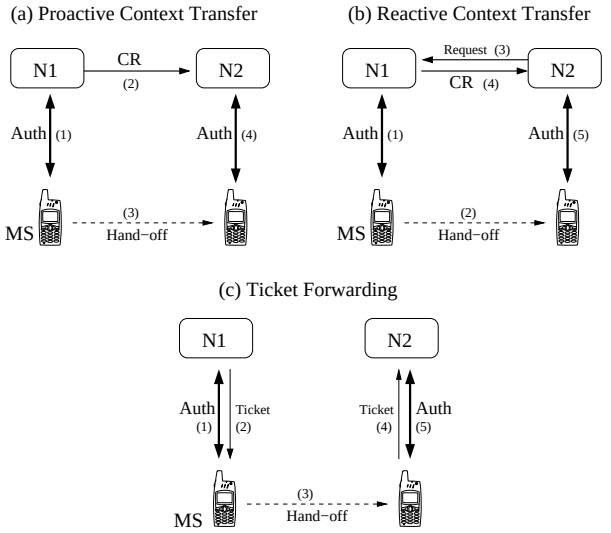

Fig. 5. *Three different chained authentication methods*

framework for secure and fast internetwork authentications. Unlike central approaches, chained authentication is a distributed method in which the authentication at the next foreign network relies on the success of authentication only at the previous network. In this section, we clarify the important assumptions of chained authentication and classify possible designs.

A. Assumptions

Assume $\{N_1, N_2, \ldots, N_m\}$, all visiting networks, is a mobility path of the client MS . When the client hands off from N_i to N_{i+1}, network N_i is called *previous network* and N_{i+1} is called *next network*. The home network of MS should be the involved with the authentication process in N_1, the first visiting network.

For chained authentication to work, adjacent pairs of networks, N_i and N_{i+1}, should hold a trust relationship. By *trust*, we mean that N_{i+1} believes that N_i provides N_{i+1} with correct information and that the authentication system and confidentiality of cryptographic keys of N_i is secure. Also, a secure channel between trusted networks exists.

Note that if the security of N_i is compromised, subsequent sessions in the following networks can be also compromised.

B. Classification

In general, the authentication process takes the following steps. To authenticate each other, the client and the authentication server exchange some messages and verify the knowledge of secret information that is known to only themselves. Typical exchanged messages include random challenges. After verification (or as a result of the verification), they generate fresh, non-repeating and secret credentials such as session keys. Note that the generated session keys appear random to everybody except the client and authentication server, i.e. no attacker can predict the secret key better than random guessing. Moreover, client and server share the session key, and the server only needs to give a hash of the key to the next server so that the next server and the client share the same secret key without any message exchanges involved.

In this section, we introduce two criteria for chained authentication methods, and we derive three categories based on those criteria.

1) context transfer or ticket forwarding: We define context as the secret material of the previous network, or a hash of it, which enables the next network to establish a security association with the client without having to perform the entire authentication protocol from the scratch [27]. Either the authentication server can deliver the context directly, or the client can deliver the context via ticket. The first method, called *context transfer*, requires a secure channel between servers, usually over the wire. In the second method, called *ticket forwarding*, the previous network N_i issues a ticket to the client. The ticket contains the context and expiration time, encrypted so that only receiving network N_{i+1} can decrypt. The client receives the ticket from N_i, and tenders it to N_{i+1}. Kerberos is an example of an authentication system that also makes use of tickets [25]. The following describes how a ticket is issued and forwarded.

Denote client, previous AS, and next AS as c, p, and n, respectively. Let c and p share secret key $K_{c,p}$ as a result of authentication, and let p and n share $K_{p,n}$. The ticket delivery protocol looks as follows :

$$\begin{aligned} p \longrightarrow c \quad &: \quad E_{K_{c,p}}(n, T_{exp}) \mid\mid ticket \\ c \longrightarrow n \quad &: \quad ticket \end{aligned} \tag{1}$$

where $ticket = E_{K_{p,n}}(c, T_{exp}, CR)$, CR is the credential delivered, T_{exp} is ticket expiration time and $E_{K_{p,n}}()$ is an encryption procedure using secret key $K_{p,n}$.

2) reactive or proactive context transfer: The criteria in this section only apply to context transfer as described above. If the transfer happens before the hand-off, it's called *proactive*. When proactive transfer is not allowed, *reactive* context transfer can be requested to N_i by N_{i+1} after the client hand-off. It is obvious that the proactive method requires fewer authentication messages than the reactive one. However, to know which network will be next network prior to hand-off, the proactive method

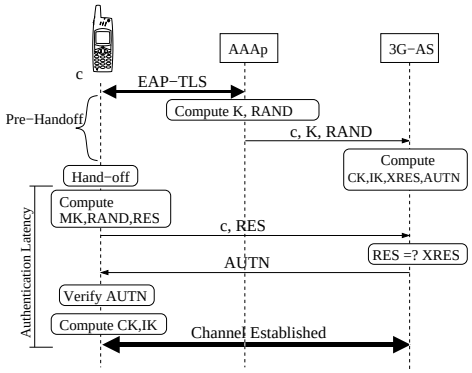

Fig. 6. *Proactive Context Transfer To 3G-AKA*

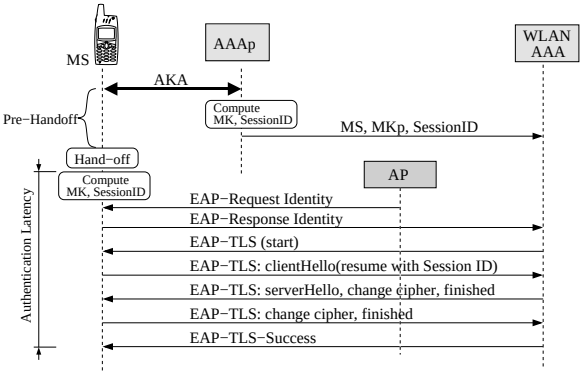

Fig. 7. *Proactive Context Transfer To WLAN(EAP-TLS)*

requires some prediction mechanism. We discuss this problem in section VI. With reactive method, even if the client left the network, the server should keep the client's credentials in its cache for some time during which the next network may request for transfer.

3) categories: Based on the aforementioned two criteria, we can categorize chained authentication methods as follows,

i) Proactive context transfer
ii) Reactive context transfer
iii) Ticket forwarding

The Fig. 5 illustrates the categorization. In the figure, The number in parentheses represents the sequence of events.

4) number of security associations: In centralized methods, since each visiting network should maintain security associations with all other home networks, $O(N^2)$ number of security associations are required where there are N different networks. However, under chained authentication methods, the number of trust relationships required is $O(N)$ without dedicated central authority such as AAA-broker [10] or identity providers [28]. The reason is the following. Let a graph $G =< V, E >$ be the neighbor graph between networks where V is the set of N networks and E is the set of edges. Since each node need to maintain security associations only with adjacent nodes, the total number of security associations is the number of edges, $|E|$. Assuming that the maximum degree is bounded by a constant e [16], $O(|E|) = O(eN) = O(N)$.

IV. Design of chained authentication method under 3G/WLAN interworking

In this section, we provide the design of chained authentication protocols under 3G and WLAN, which fall into aforementioned categories. We assume 3G and WLAN authenticate clients by AKA and EAP-TLS, respectively.

A. Proactive Context Transfer

1) Toward 3G: Figure 6 illustrates a proactive context transfer when the destination network is a 3G system. As a result of authentication, $AAAp$ (previous AAA server) and c (client) share several secret materials that are known only to themselves. For example, when previous network is WLAN, the client and $AAAp$ share a 48 byte master key, and encryption and MAC keys of 32 bytes for each direction. After authentication, $AAAp$ generates the secret key (K) and random number ($RAND$) as follows,

$$\begin{aligned} CR_{new} &= PRF_{256}(CR_{old}, \text{"3G context"}, c, N_{new}) \\ K &= CR_{new}[0...127] \\ RAND &= CR_{new}[128...255] \end{aligned}$$

where CR_{old} represents the concatenation of one or more credentials from previous authentication, N_{new} is the identification of the destination network, and c is the client's identification, such as IMSI (International Mobile Subscriber identity). After receiving c, K and $RAND$, 3G-AS (the authentication server of destination 3G system) computes CK, IK, $AUTN$, and $XRES$. Note that AMF, AK and SQN is not sent even though they are needed for generation of $AUTN$ because the 3G-AS can pick them on its own[3]. After the client hands off to network N_{new}, it computes MK and $RAND$, derives RES, and provides RES to 3G-AS along with a registration request. 3G-AS, who already has $XRES$, verifies RES from the client and sends $AUTN$ as a proof of authenticity. After client succeeds in verifying $AUTN$, a secure channel is established.

[3] AK can be any user-dependent random number and AMF can be set by 3G-AS. If the previous network is 3G, SQN can be also sent to avoid synchronization failure. Even if the previous network is non-3G, 3G-AS can avoid synchronization problem by using a new array index. See Annex C in [29]

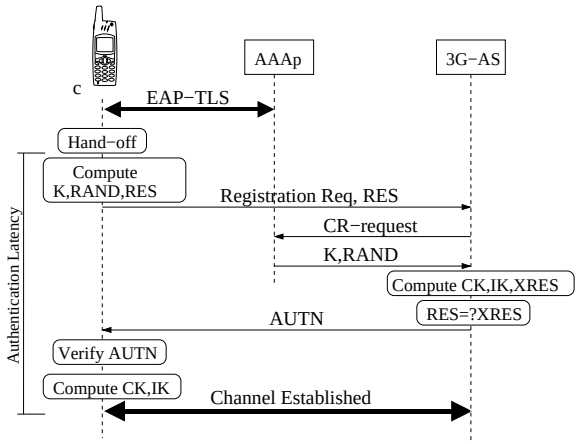

Fig. 8. *Reactive Context Transfer To 3G-AKA*

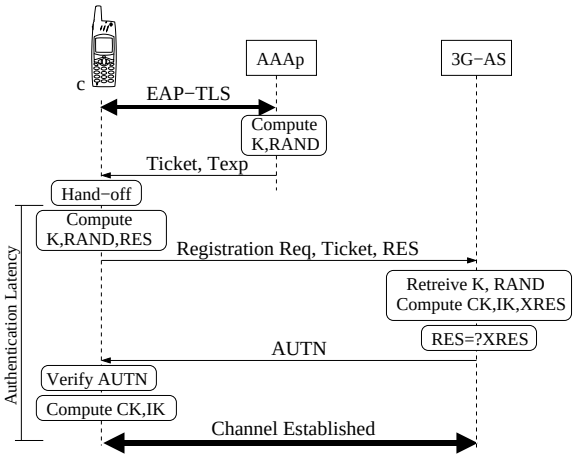

Fig. 10. *Ticket Forwarding To 3G-AKA*

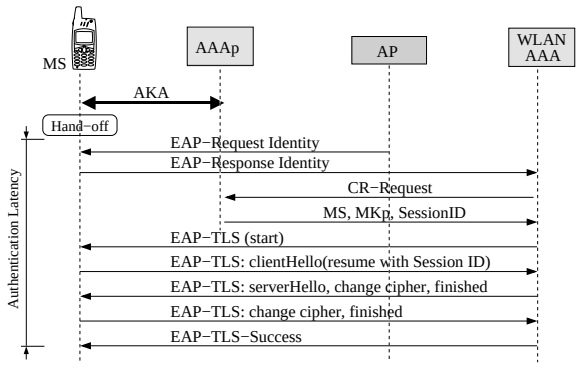

Fig. 9. *Reactive Context Transfer To WLAN(EAP-TLS)*

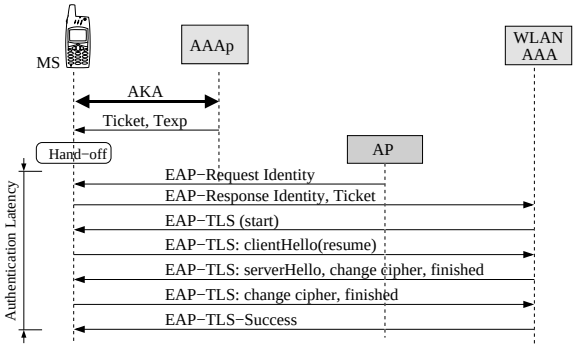

Fig. 11. *Ticket Forwarding To WLAN(EAP-TLS)*

2) Toward WLAN: Figure 7 illustrates a proactive context transfer when the destination network is a WLAN system. EAP-TLS supports the resume process which allows the server and the client to skip master key generation and to resume a previously established association. The TLS session resume requires a 48 byte master key (MK) and 32 byte session ID ($sessionID$), generated as follows:

$$\begin{aligned} CR_{new} &= PRF_{640}(CR_{old}, \text{"WLAN context"}, c, N_{new}) \\ MK &= CR_{new}[0...384] \\ RAND &= CR_{new}[389...639] \end{aligned}$$

Before the hand-off, MK and $sessionID$ is transferred to the new network. When the client requests the resumed session with the $clientHello$ message, the WLAN-AAA server can identify the requested $sessionID$ from its cache and allow the client to resume the previous session.

B. Reactive Context Transfer

Reactive context transfers are almost identical to proactive ones except for the timing of the transfer and the initiating party. The context is identical to proactive case. After MS hands off to the new network, the new network's authentication server requests the previous network to send the context for the MS. For message diagrams of the reactive cases, see figures 8 and 9.

C. Ticket Forwarding

The context included in the ticket is also identical to context transfer methods. The created context CR_{new} is included in a ticket, whose construction is in equation (1) in section III-B, and forwarded. We assume that the ticket is tendered to the next authentication server in *registration request* for 3G (Fig. 10) and in *EAP-Response Identity* message for WLAN system (Fig. 11), respectively.

D. Trade-off between performance and security

Although our schemes use specific contexts, such as $(K, RAND)$ for 3G and $(MK, SessionID)$ for WLAN, many other choices for context exist, each with their own performance and security tradeoffs. For example, the context could be a fresh session key for the new secure channel. The resulting scheme requires

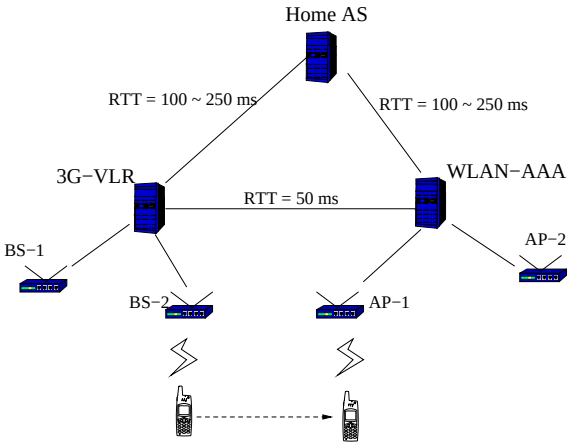

Fig. 12. *Testbed configuration*

no authentication protocol, resulting in a very fast hand-off. However, it requires an unusually strong trust relationship between networks – highly unlikely between different business domains. At the opposite end of the spectrum, the destination network may not trust the previous network much at all, and require that a compromise of the previous session, or context, cannot pose a threat to security at the destination network. For this purpose, the destination network would have to possess a pre-shared secret key with the client, which is possible under multi-homed environment. The schemes proposed in this paper require moderate trust relationship between networks, provide moderate performance gain, and are suitable for single-homed clients.

V. Experiments and results

We implemented the chained authentication algorithms discussed in section IV to simulate 3G-WLAN internetwork authentication on an indoor 802.11b wireless network. Below, we present the testbed setup, implementation, measurement methodology, and experimental results.

A. Testbed

We present the testbed for our experiment in figure 12. The three AAA servers simulate authentication servers at the home network (HomeAS), 3G network (3G-VLR) and WLAN network (WLAN-AAA). 3G base stations are simulated by 802.11b access points. Using NIST Net emulator [30], we set the RTTs (Round Trip Time) between servers as shown in the figure (with standard deviation of 2ms) to simulate the distance between different networks[4]. Table I shows the hardware specifications of the testbed.

[4][31] and [32] used 100ms to 200ms for RTT between Foreign Agent and Home Agent in Mobile IP

TABLE I
Testbed Hardware Configuration

Entity	Processor	Mem	OS
MS	AMD 1.3 GHz	512 MB	Linux
AP	AMD 133 MHz	64 MB	OpenBSD
HomeAS	P-III 800 MHz	128 MB	Linux
3G-VLR	P-III 933 MHz	512 MB	Linux
WLAN-AAA	P-III 550 MHz	128 MB	Linux

B. Implementation

We emulate 3G authentication over 802.11b by implementing 3G-AKA protocol over EAP[5]. We implemented cryptographic functions such as f0, f1, etc, from the sample implementation in [18]. The mobile station runs a modified version of Open1x Xsupplicant [33] on Linux 2.4.25. The modifications include client-side AKA implementation, and the ability to store contexts and tickets for chained authentication. The AP and BS run Open1x authenticator on OpenBSD 3.3 [33]. The authentication servers run a modified FreeRADIUS on Linux 2.4.18. These modifications include the ability to transfer contexts between AS's in proactive or reactive authentication, to issue and decrypt tickets, to perform TLS resume, and to perform the server-side AKA state machine.

C. Measurement

For original (centralized) authentication, we performed 60 hand-offs each for 100 ms, 150 ms , 200 ms, and 250 ms latency settings between 3G-VLR/WLAN-AAA and HomeAS. For each chained authentication algorithm, we performed 60 hand-offs between 3G and WLAN networks. We measured the authentication latencies by sniffing the wireless medium and by capturing RADIUS packets between servers using tcpdump [34]. Computation overhead was measured by internal time loggings.

D. Results

In this section, we analyze the experimental results with respect to authentication latencies and the overheads of chained methods. In brief, the results show that proactive context transfer and ticket forwarding reduce the AKA latency to 36.8% and EAP-TLS latency to 23.1% when RTT between visiting and home networks is 200 ms. Also, the overhead for chained methods was minimal.

[5]Note that AKA of 3G differs from EAP-AKA defined in [12]

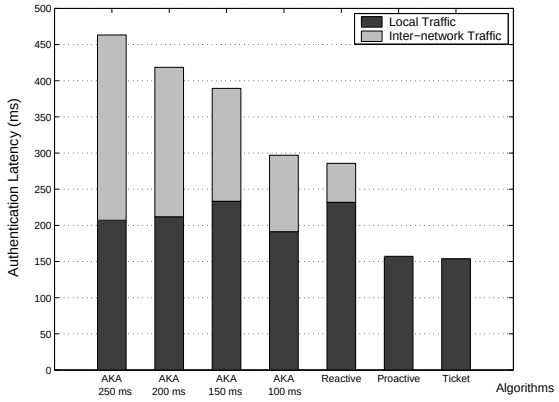

Fig. 13. *Authentication Latencies in 3G*

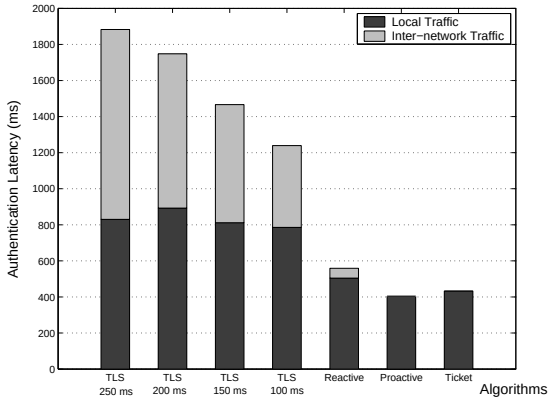

Fig. 14. *Authentication Latencies in WLAN*

1) authentication performance: The measurement results show that proactive context transfer and ticket forwarding reduce the AKA latency to 36.8% and EAP-TLS latency to 23.1% when RTT between visiting and home networks (FAAA-to-HAAA RTT) is 200 ms. Figure 13 compares the authentication latencies of tested algorithms when the destination network is 3G. As seen in the graph, AKA takes from 297.0 ms up to 463.2 ms when the FAAA-to-HAAA RTT is from 100 ms to 250 ms, respectively. The bright portion of the bars represent the time spent for communications beyond the current network (internetwork traffic). Note that proactive and ticket methods do not require any internetwork traffic during the hand-off. As far as authentication latency is concerned, proactive and ticket method achieve the same performance.

Figure 14 compares the performance toward WLAN network. Original EAP-TLS takes from 1238.98 ms up to 1882.98 ms when FAAA-to-HAAA is 100 ms to 250 ms, respectively. In contrast to AKA, each EAP-TLS message has to reach the home AAA server, so the reduction of authentication latency by chained methods is much more apparent in WLAN.

2) overhead: Proactive context transfer introduces overhead in the form of wired communications between AAA servers. The amount of the overhead is a product of the number of neighbors and the size of context. Also, the proactive method requires memory for context caching at the destination network. The duration of such memory usage should be at least the average internetwork hand-off interval. For reactive methods, the previous AAA needs to keep the context of a departed client long enough so that it can respond to context requests on behalf of that client. The computation overhead of ticket forwarding includes the generation and interpretation of the ticket, which involves shared-key encryption. We found the ticket generation time on the previous server and ticket interpretation time on the destination server to be less than 1 ms each. Furthermore, ticket forwarding imposes traffic overhead proportional to the ticket size (80 bytes for a WLAN ticket, and 32 bytes for a 3G ticket).

VI. Soft-Prediction of next network

As described in section III, the current authentication server needs to know where to send context before the client hands off. For this purpose, the authentication server must either predict the destination network to which the client will hand off, or predict a set of potential destination networks. We call this *soft-prediction*. In this section, we propose a soft-prediction system using hierarchical neighbor graph.

A. Neighbor Graphs

Neighbor graph is a dynamic, distributed data structure that abstracts hand-off relationships between access points in a WLAN [15] [16]. A neighbor graph is generated based on continuous observation of actual hand-offs in the network. When a mobile station hands off from one access point to another, both access points realize the hand-off relationship between them. This realization is possible by IAPP (Inter-Access Point Protocol) defined in IEEE Draft 802.11f [35]. By observation, each access point *learns* and maintains the list of neighbor access points to which some mobile station has handed off.

The neighbor graph is a distributed data structure because each access point only stores the local topology. The distributed nature of neighbor graph guarantees scalability, minimal memory usage and memory-access delay. The neighbor graph is dynamic because it can adapt to the changing mobility patterns of the users. As the user's mobility habit changes, the neighbor graph adds new edges or deletes obsolete edges to more closely reflect current hand-off relationships.

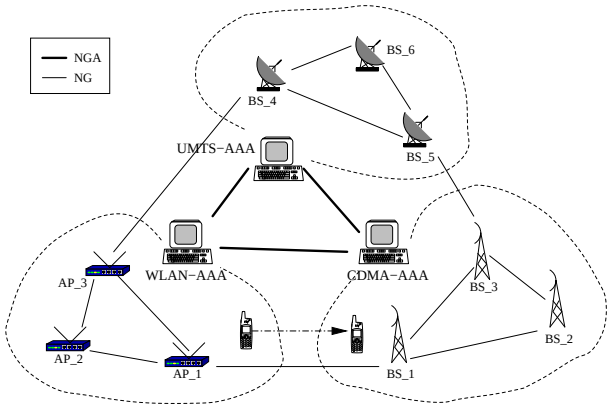

Fig. 15. *Neighbor Graph for Internetworking*

Another advantage of neighbor graph is that it provides a highly accurate method of identifying potential next access points to which the mobile station will hand off. Reference [15] shows that neighbor graph provides an order of magnitude reduction in the layer 2 hand-off latency incurred by context transfer between old and new access points. The effect of this approach improves dramatically as user mobility increases. Reference [9] shows how neighbor graphs can be utilized to obtain a 99% reduction in authentication time of an IEEE 802.11 hand-off (full EAP-TLS) by proactively distributing necessary key material one hop ahead of the mobile user. Also reference [16] shows another application of NG, in which the station can reduce probing latency by up to 84%.

B. Hierarchical Neighbor Graphs

Although NG was originally suggested to be used for abstracting hand-off relationships inside a network, it can be extended to the internetwork environment. We call this internetwork generalization of neighbor graph Hierarchical Neighbor Graph (HNG).

The following defines the HNG. Let the base neighbor graph,

$$NG_b \quad = \quad < V_b, E_b >$$

where V_b = $\{$ $N_1, N_2, \ldots, N_n$ $\}$ and E_b = $\{$ $< N_i, N_j >$: a mobile can hand off from N_i to N_j $\}$. Given a set partition of V_b, $\{P_1, P_2, \ldots, P_k\}$ where k is the number of partitions, we can generate another neighbor graph of higher level,

$$NG_h =< V_h, E_h >$$

such that V_h = $\{$ $P_1, P_2, \ldots, P_k$ $\}$ and E_h = $\{$ $< P_i, P_j >$: there exist $U \in P_i$ and $V \in P_j$ such that $< U, V > \in E_b$ $\}$.

The set of neighbor graphs on different levels defines a hierarchical neighbor graph, HNG = $\{$ NG_b, NG_h $\}$.

In the 3G/WLAN scenario, each base node N_i represents an access point in WLAN or a base station in 3G (Fig. 15). A partition is an individual network with its own authentication system. Thus, P_i represents the authentication server of the ith network. Although we define a two level hierarchical neighbor graph for simple explanation, HNG can easily be expanded to multiple levels.

By the definition above, NG_h and HNG can be generated from NG_b and the set partition. The generation method inside a network uses inter-AP communication methods, such as IAPP [35] in [15]. However, we cannot apply such mechanisms directly to learn an edge between heterogeneous networks. Since there are no trivial means of communication between heterogeneous base nodes (e.g. between WLAN access points and 3G base stations), the involvement of higher level entities, i.e. authentication servers, is required in the generation process.

C. scalability of hierarchical neighbor graph

Since the number of users under a higher level node is the aggregation of underlying lower level nodes, the scalability problem can be an issue in hierarchical neighbor graphs. It would be wasteful for a AAA to proactively transfer contexts to all neighboring AAA's. To address this problem, the AAA must be aware of the topology within the network. In Fig. 15, WLAN has two neighbors UMTS and CDMA. However, AP_2 has no internetwork neighbor and AP_1 and AP_3 each have one internetwork neighbor. Therefore, WLAN-AAA should use AP's with internetwork neighbors for proactive caching, rather than using all AP's WLAN. For example, when the mobile station associates to AP_3, WLAN-AAA should only proactively transfer the context to UMTS. No context transfer is required for clients under AP_2. In this way, we can make hierarchical neighbor graph more scalable by allowing AAA's to make more informed decisions about where to send contexts.

VII. Related Work

Previous research on internetwork authentication mostly involved *centralized approaches*, where a single authentication server on the home network authenticates the client. In such approaches, the basic authentication model is the following: Assume MS, whose home network is N_h, is visiting a foreign network N_f. Denote the authentication servers in N_h and N_f as AS_h and AS_f, respectively. Most authentication schemes in such

environments require the MS to authenticate itself to AS_h through AS_f [10] [11] [12] [13] [14] [6]. 3G wireless communication systems such as GSM, UMTS, and CDMA2000 already have such authentication mechanisms in place [29] [17]. Reference [11], [12], and [36] are adapting 3G-like mechanisms into the WLAN security using EAP [23] under a AAA framework [22] [37]. However, these schemes still suffer performance degradation when there is high latency between the AS_f and AS_h.

To reduce the number of messages exchanged between AS_f and AS_h, which tend to be located very far apart, reference [36] and [38] suggest using a 3G style authentication mechanism by introducing AAA-broker servers on the path from AS_f to AS_h. The limitation of their method is that their framework can only use simple challenge-response based authentication protocols. Furthermore, the trust relationships between all the brokers with home networks faces a scalability problem.

The number of security associations is another issue in the wide-area wireless network environment. When foreign and home networks collaborate, secure associations between networks are necessary, resulting in a total of $O(N^2)$ security associations. Reference [10] attempts to address this problem by introducing a dedicated AAA server (called the AAA-broker) which maintains the security associations with all the networks and provides broker service between foreign and home networks. This scheme reduces the total number of security associations down to $O(N)$. However, since one broker handles all authentication requests, it suffers from a scalability problem as well as the poor performance caused by triangular routing via AAA-broker.

Unlike previous approaches, context transfer schemes can avoid the message exchanges with the home network during hand-off. Although research about intra-domain context transfer can be found in literature [39] [40] [15], to our best knowledge, research on inter-domain context transfer scheme is rare. Instead of authenticating through the home network, reference [41] proposed AAA context transfer between gateways to eliminate the interactions between mobile host and home AAA server in All-IP infrastructures. This is a reactive method which happens after hand-off and it requires modifications at routers. Also, the context simply consists of session keys, and the strongest of trust relationships is required between networks.

[25] and [28] have proposed a different method of delivering context to next network: let the client forward the context. Kerberos [25] uses an *access grant ticket* for this purpose whereas [28] uses a *cookie*. Kerberos is a distributed authentication service that allows a client to prove its identity to a server, called verifier, without sending data across the network [42]. Rather than sending data directly to the next network, the authentication server issues the client a ticket which carries the new session key and expiration time to be used in the next network. The authentication server signs the ticket itself and encrypts it by a secret key shared with the next network. However, Kerberos is another form of centralized authentication because the home authentication server should get involved in the issuance of tickets, and the client needs a ticket for every network it visits. Furthermore, the weakness of the Kerberos password system is identified in [43]. In this paper, we show that moving the ticket issuance authority from the home network to the previous visiting network constitutes a chained authentication method. Single sign-on (SSO) scheme [28] enables users to access multiple systems with single authentication, but it is limited to web-based authentication using cookies.

VIII. Conclusion and Future Work

In this paper, we defined chained internetwork authentication schemes as distributed methods in which the authentication at each visiting network relies on the established security association in the previous visiting network. We emphasized that chained authentication methods can achieve efficiency and security at the same time. Their distributed characteristics also reduce the required trust relationships throughout wide area wireless networks to $O(N)$, where N is the number of networks. Our experiments showed that *proactive context transfer* and *ticket forwarding* reduced the 3G authentication latency to 36.8% and WLAN EAP-TLS latency to 23.1% when RTT between visiting and home networks is 200 ms. The performance benefit of such schemes grow as the distance to home network increases.

For proactive context transfer to be a scalable and feasible solution, more investigation about the soft-prediction scheme is needed. The optimization of HNG under heterogeneous environments is to be studied and manifested. Furthermore, the derivative problems from chained authentication, such as accounting, the use of multi-homed clients, and mixture of centralized and chained methods will be studied.

References

[1] "Bluetooth specifi cation," http://www.bluetooth.org/spec/, 2001.
[2] Salkintzis, Ke. et al., "WLAN-GPRS Integration for Next-Generation Mobile Data Networks," *IEEE Wireless Communications*, Oct. 2002.

[3] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa, "Wireless LAN Access Network Architecture for Mobile Operators," *IEEE Communications Magazine*, pp. 82–89, Nov. 2001.

[4] Pahlavan, K. et al., "Handoff in Hybrid Mobile Data Networks," *IEEE Personal Communications*, Apr. 2000.

[5] M. Buddhikot, G. Chandranmenon G., S. Han, Y. W. Lee, S. Miller S., and L.Salgarelli, "Integration of 802.11 and Third Generation Wireless Data Networks," *IEEE INFOCOM 2003*, Apr. 2003.

[6] M. Buddhikot and G. Chandranmenon and Seungjae Han and Yui-Wah Lee and S. Miller and L. Salgarelli, "Design and Implementation of a WLAN/CDMA2000 Interworking Architecture," *IEEE Communications Magazine*, Nov. 2003.

[7] Third Generation Partnership Project, "3GPP system to Wireles Local Area Network (WLAN) interworking; System description, TS 23.234, v6.0.0," *3GPP2 Techinical Specifications*, Apr. 2004.

[8] Third Generation Partnership Project, "Digital cellular telecommunications system (Phase 2+); Performance Requirements on Mobile Radio Interface, TS 44.013 v5.0.0, R5," *3GPP Techinical Specifications*, June 2002.

[9] Arunesh Mishra, Minho Shin, Jr. Nick L. Petroni, T. Charles Clancy, and William A. Arbaugh, "Pro-active Key Distribution using Neighbor Graphs," *IEEE Wireless Communications Magazine*, Feb. 2004.

[10] Luca Salgarelli, Milind Buddhikot, Juan Garay, Sarvar Patel, and Scott Miller, "Efficient Authentication and Key Distribution in Wireless IP Networks," *IEEE Wireless Communications Magazine*, Nov. 2003.

[11] H. Haverinen, "EAP SIM Authentication," *Work in progress - Internet Draft, IETF, draft-arkko-pppext-eap-sim-03.txt*, Feb. 2002.

[12] J. Arkko and H. Haverinen, "EAP AKA Authentication," *Work in progress - Internet Draft, IETF, draft-arkko-pppext-eap-aka-12.txt*, Apr. 2004.

[13] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)," *Work in progress - Internet Draft, IETF. draft-ietf-pppext-eap-ttls-03.txt*, Aug. 2003.

[14] R. Molva, D. Samfat, and G. Tsudik, "Authentication of Mobile users," *IEEE Networks*, vol. 8, no. 2, 1994.

[15] Arunesh Mishra, Minho Shin, and William A. Arbaugh, "Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network," in *IEEE Infocom 2004*, Mar. 2004.

[16] Minho Shin, Arunesh Mishra, and William A. Arbaugh, "Improving the Latency of 802.11 Hand-offs using Neighbor Graphs," in *To appear in Mobisys 2004*, June 2004.

[17] Geir Koien and G. Rose, "Access security in CDMA2000, including a comparison with UMTS access security," *IEEE Wireless Communications Magazine*, pp. 19–25, Feb. 2004.

[18] 3GPP2, "3gpp2 s.s0055 version 1.0, enhanced cryptographic algorithms," *3GPP2 Techinical Specifications*, Jan. 2002.

[19] William A. Arbaugh, Narendar Shankar, and Justin Wang, "Your 802.11 Network has no Clothes," in *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*, December 2001.

[20] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, "Using the fluhrer, mantin, and shamir attack to break wep," in *Network and Distributed System Security Symposium (NDSS)*, 2002.

[21] IEEE, "Draft Amendment to STANDARD FOR Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements. Part 11: Wireless Medium Access Control and Physical Layer(PHY) Specifications: Medium Access Control (MAC) Security Enhancements," *IEEE Standard 802.11i*, May 2003.

[22] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000.

[23] L. Blunk and J. Vollbrecht, "Ppp extensible authentication protocol (eap)," *RFC 2284*, March 1998.

[24] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," *RFC 2246*, Jan. 1999.

[25] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," *RFC 1510*, 1993.

[26] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," *RFC 2716*, October 1999.

[27] J. Kempf, "Problem Description: Reason For Performaing Context Transfers Between Nodes in an IP Access Network," RFC 3374, 2002.

[28] Yasuhiko Matsunaga, Ana Sanz Merino, Takashi Suzuki, and Randy H. Katz, "Secure Authentication System for Public WLAN Roaming," in *Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH)*. 2003, pp. 113–121, ACM Press.

[29] Third Generation Partnership Project, "3G Security; Security architecture (Release 6), 3GPP TS 33.102 v6.0.0," *3GPP Techinical Specifications*, Sept. 2003.

[30] "Nist net simulator," http://snad.ncsl.nist.gov/itg/nistnet/.

[31] A. Festag and A. Wolisz, "Performance Evaluation of Mobile IP: Investigating the Concept of Hierarchical Foreign Agents," in *In Proceedings of Mobility for All-IP Networks - Mobile IP (MAIN 2001)*, Apr. 2001.

[32] Robert Hsieh and Aruna Seneviratne, "A comparison of mechanisms for improving mobile IP handoff latency for end-to-end TCP," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*. 2003, pp. 29–41, ACM Press.

[33] "Open1x," http://www.open1x.org.

[34] "tcpdump," http://www.tcpdump.org.

[35] IEEE, "Draft 5 Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," *IEEE Draft 802.11f/D5*, January 2003.

[36] Hahnsang Kim and Hossam Afifi, "Improving Mobile Authentication with New AAA Protocols," in *Proceedings of IEEE ICC (International Conference on Communications), Anchorage, USA*, May 2003.

[37] Pat R. Calhoun, Glen Zorn, Ping Pan, and Haseeb Akhtar, "Diameter Framework Document," Internet-Draft, draft-ietf-aaa-diameter-framework-09.txt, February 2001, Work in progress.

[38] Hahnsang Kim, Walid Ben-Ameur, and Hossam Afifi, "Toward Efficient Mobile Authentication in Wireless Inter-domain," in *Proceedings of IEEE ASWN (Applications and Services in Wireless Networks), Berne, Switzerland*, 2003.

[39] R. Koodli and C.E. Perkins, "Fast Handover and Context Relocation in Mobile Networks," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 5, October 2001.

[40] M. Nakhjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol," *Internet Draft : draft-ietf-seamoby-ctp-01.txt*, March 2003.

[41] Georgiades M, N. Akhtar, C. Politis, and R. Tafazolli, "AAA Context Transfer for Seamless and Secure Multimedia Services," *European Wireless 2004, Barcelona,Spain*, Feb. 2004.

[42] B. Clifford Neuman and Theodore Ts'o, "Kerberos: An authentication service for computer networks," *IEEE Communications*, vol. 32, no. 9, September 1994.

[43] Thomas Wu, "A Real-World Analysis of Kerberos Password Security," in *Proceedings of NDSS (Network and Distributed System Security Symposium), San Diego, California*, Feb. 2003.