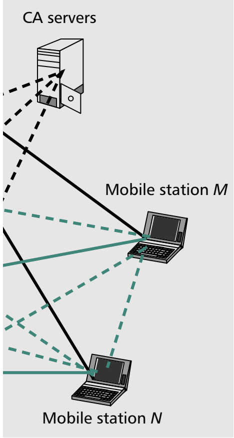
IEEE802.11 ROAMING AND AUTHENTICATION IN WIRELESS LAN/CELLULAR MOBILE NETWORKS

MINGHUI SHI, XUEMIN (SHERMAN) SHEN, AND JON W. MARK, UNIVERSITY OF WATERLOO



A proposed wireless LAN service integration architecture is based on current wireless LAN hotspots, making migration to new service easier and cost effective. The proposed architecture offers wireless LAN seamless roaming in wireless LAN/Cellular Mobile Networks.

ABSTRACT

A wireless LAN service integration architecture based on current wireless LAN hot spots is proposed so that migration to a new service becomes easier and cost effective. The proposed architecture offers wireless LAN seamless roaming in wireless LAN/cellular mobile networks. In addition, a link-layer-assisted Mobile IP handoff mechanism is introduced to improve the network/domain switching quality in terms of handoff delay and packet loss. An application layer end-to-end authentication and key negotiation scheme is proposed to overcome the open air connection problem existing in wireless LAN deployment. The scheme provides a general solution for Internet applications running on a mobile station under various authentication scenarios and keeps the communications private to other wireless LAN users and foreign networks. A functional demonstration of the scheme is given. The research results can contribute to rapid deployment of wireless LANs.

INTRODUCTION

IEEE 802.11b, or Wi-Fi, compatible products have become a de facto standard component in mobile devices. An increasing number of wireless Internet access services have been appearing in places such as airports, cafes, and bookstores. Annual industry revenues already exceed US$1 billion, and is expected to pass US$4 billion by 2007 [1]. In addition, mobile devices with both cellular phone and Wi-Fi capability are coming. Demand for integrating multiple mobile computing services into a single entity is preeminent.

Figure 1 shows a global architecture of the public wireless Internet. Mobile IP is used throughout the architecture to support user roaming. Wi-Fi-based hotspots could be adjacent or distributed in cellular networks. When the services of wireless LAN and cellular network are integrated, the mobile station can move across those networks. There are two types of roaming: roaming between wireless LANs is defined as *horizontal* roaming; roaming between a wireless LAN and a cellular network is defined as *vertical* roaming. This article focuses on proposing a high-performance secure cellular-network-integratable wireless LAN service framework.

Many wireless Internet service providers (WISPs), such as T-mobile, provide public wireless LAN Internet access at hot spots using a network access server (NAS). The NAS allows only legitimate customers to use the service and provides intradomain roaming because the hot spots from one WISP share the same customer base. However, it lacks an architecture to provide interdomain roaming and Mobile IP support. A user cannot access hot spots of service provider B with his/her account from A, even though A and B would like to have a roaming agreement.

In internetworking implementation, handoff performance should also be considered. Mobile IP handoff delay can be divided into two elements: movement detection and signaling for registration. Several proposed approaches are actually only effective on registration signaling delays. For instance, a micro-mobility approach [2] divides a network in a hierarchical manner, and location management is handled locally when the mobile station moves within a smaller area at the lower hierarchy level. Another approach is simultaneous binding [3], in which multiple care-of address bindings for the mobile station are maintained and packets destined for the mobile station are transmitted to all care-of addresses to reduce packet loss during handoff. However, it cannot be used in an IEEE802.11 network, because current wireless LAN cards can only access one access point or channel at a time.

On the other hand, Wired Equivalency Protocol (WEP) has several problems in both transmission privacy and deployment. Various studies show that WEP is vulnerable to several attacks [4, 5], especially in a heavily loaded wireless network. WEP uses a single key shared between the access point and clients. Malicious clients are able to tap into the communication traffic of other clients who are associated with the same access point. Most hotspots do not use data encryption due to this technical limitation. Authentication can be used to negotiate a shared session key to further encrypt data traffic in the session [6–9]. Although there are many authentication schemes published, they do not generally

1536-1284/04/$20.00 © 2004 IEEE

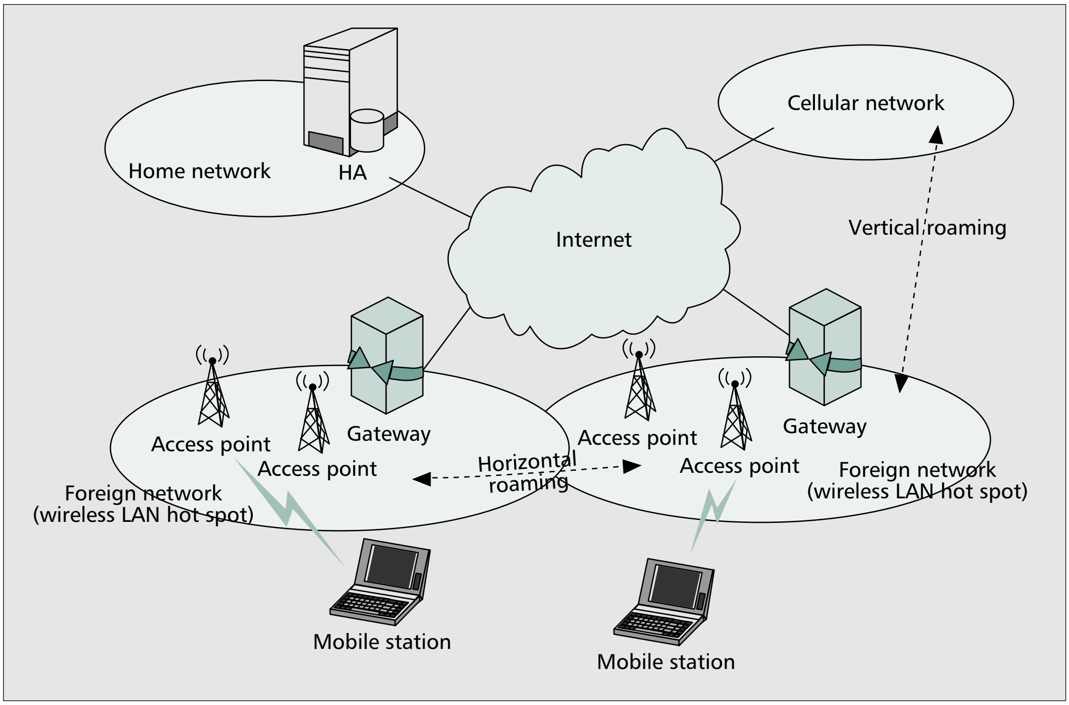


Figure 1. *Wireless service integration architecture*

Since 3G and beyond cellular networks use or very likely will continue to use AAA structure and protocol to control network access and manage user accounts, the IEEE802.11 roaming architecture and signaling processes should work with cellular networks.

support Internet applications for wireless mobile devices. For example, the authentication schemes proposed in [10–12] allow a mobile station to communicate to another one directly, but there is no solution for a mobile station to communicate with a fixed Internet server, which is found in ftp applications.

Protected transmission based on Secure Shell (SSH) and/or Secure Sockets Layer (SSL) is suggested to secure wireless transmission. SSH requires a previously generated public/private key pair, so it could never be applied to authentication between parties who have not contacted each other before. SSL is not suitable for extension to mobile wireless Internet either, because the operation of SSL relies on certification verification by certificate authority (CA) servers. It is not practical for CA servers to store the certificate of every mobile station because the number of mobile stations is too large (for the same reaso, client authentication in SSL is optional). The home network would not like to register every mobile station to CA servers either. In the case of a wireless LAN hot spot, the service access is controlled by medium access control (MAC) addresses of the mobile stations. Usually there is no key negotiation during the network authentication and Mobile IP registration phases.

The objective of this work is to propose a secure wireless LAN service integration architecture and necessary signaling process design. These issues are divided into three categories:

IEEE802.11 service integration functionality: The architecture should be able to integrate into cellular networks. Since third-generation (3G) and beyond cellular networks use or very likely will continue to use authentication, authorization, and accounting (AAA) structure and protocol to control network access and manage user accounts, the IEEE802.11 roaming architecture and signaling processes should work with cellular networks.

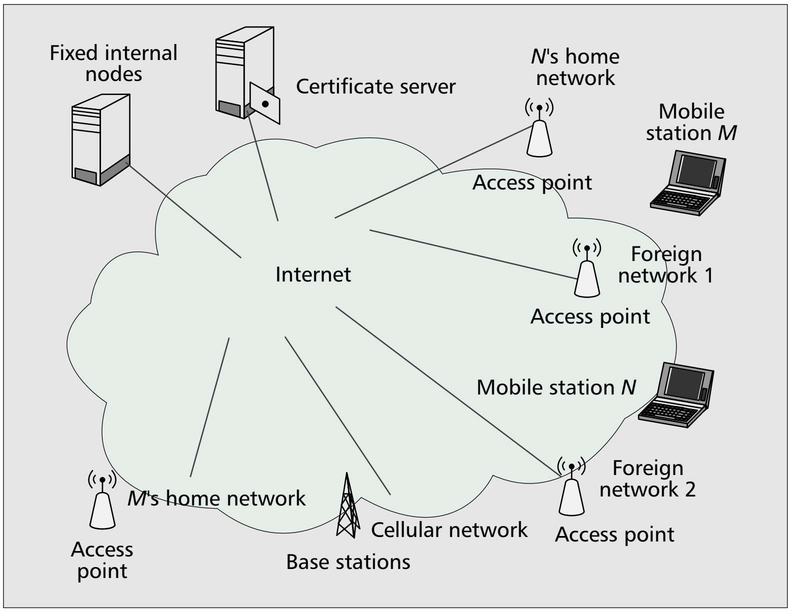
Wireless network security: The security issues include network access control, user account management, and transmission privacy. The first two items are taken care of by using the AAA structure. For the third item, a wireless LAN hot spot has no general solution to guarantee data transmission privacy due to the poor design of WEP.

Service quality: Service quality mainly refers to handoff speed and packet loss rate. Naive handoff acceleration solutions do not apply to an IEEE802.11 network interface cards, because they can only talk to one another, so solutions cannot guarantee no packet loss.

The remainder of the article is organized as follows. We present the infrastructure of wireless LAN roaming. We then give a security mechanism for wireless LAN transmission and related demonstration results, followed by a summary of the work.

IEEE 802.11 Wireless LAN Roaming

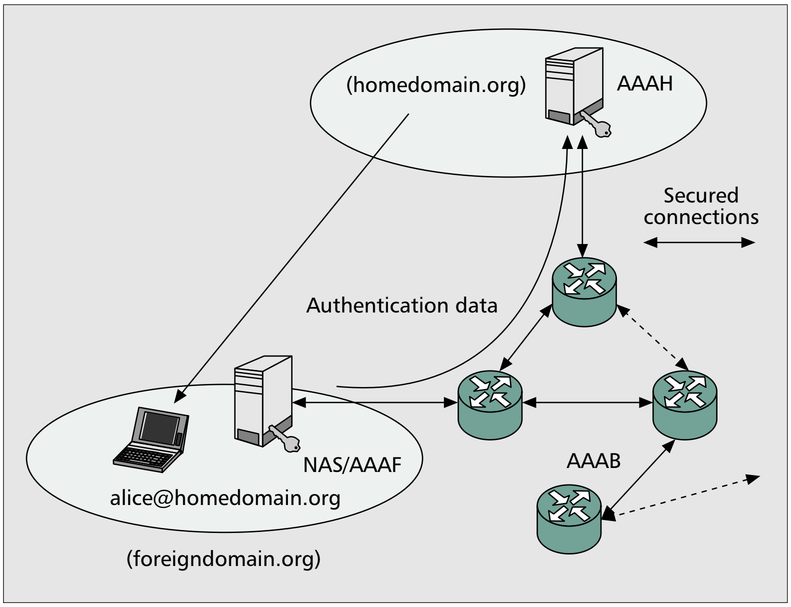
Figure 2 shows the infrastructure of the mobile networks under consideration. The Internet offers much larger bandwidth and lower transmission error rates than wireless links. The home network is considered a private network, which only allows its users access. The foreign networks are the real WISPs. After completion of a registration process, a mobile station and a corresponding foreign network will share a key for further encrypted communications. Fixed nodes represent common Web sites. Some of them need authentication before accessing. The cellular networks and base stations are 3G-based. Access points, which form a hot spot, are



■ **Figure 2.** *The proposed network structure for IEEE802.11 service integration.*

the attachment points that allow mobile stations to wirelessly access the network. A mobile station, as a member of its home network, is allowed to access the resources in the home network whenever it is within or outside the home network. CA servers are special servers that issue and verify certificates to fixed nodes or networks upon request so that they have proofs to identify themselves. CA servers are organized in a tree topology and working in a distributed way, so that it is not necessary to connect all Internet servers to one CA server. Mobile stations do not contact CA severs directly because of the large population size. CA shares independent secret key with the servers which it connects with.

The proposed IEEE802.11 roaming structure is based on an AAA broker with a Remote Authentication Dial-In User Service (RADIUS) server proxy. RADIUS is popular and easier to use for integrating hot spot service into AAA-based cellular networks. The broker model is suitable for large-scale and commercial implementation because a RADIUS server can simply have one simple security association or a presetup shared secret with the RADIUS proxy. RADIUS proxies forward authentication and accounting requests from different domains to their destination.



■ **Figure 3.** *The network structure of AAA brokers.*

The RADIUS Proxy

RADIUS servers of multiple ISPs can be interconnected via a series of forwarding servers. The RADIUS server retrieves the remote server's domain from the user's request that includes the network access identifier (NAI) [13–15] in the form of identifier@domain_name, which identifies a user's name and the domain to which he or she belongs. Then it forwards the request to the remote server identified by the domain. The remote server also replies through the forwarding server.

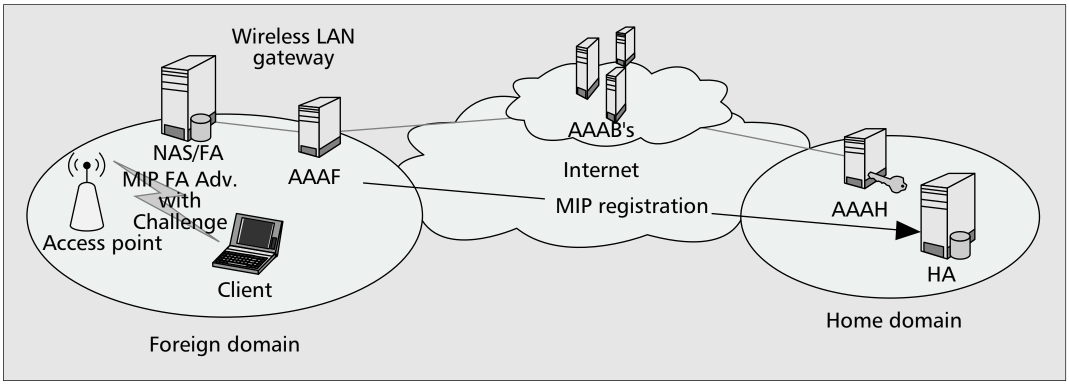
A group of forwarding servers with secured communication tunnels between each other are used as AAA brokers (AAABs). Figure 3 illustrates the network structure of AAABs. A mobile user whose NAI is alice@homedomain.org moves from its home domain to another domain (e.g., foreigndomain.org). The NAS located in the foreign domain authenticates the mobile user, and forwards this request via RADIUS protocol to the foreign AAA (AAAF). According to NAI, the AAAF forwards the request to the home AAA (AAAH) through the AAABs.

When the number of domains increases, it is no longer feasible to connect all the AAA servers to one AAAB network. The AAABs will be grouped according to geographical distribution of the network domains. In this way the complexity of each AAA broker can be reduced. The performance of an AAAB cluster is evaluated by the number of hops to forward the AAA request from the originator to the destination.

IEEE 802.11 Horizontal Roaming

The IEEE802.11 horizontal roaming architecture is shown in Fig. 4. The hot spot is connected to the Internet through a gateway. Each network domain is interconnected by AAABs. In order to provide IP mobility, the functionality of a foreign agent (FA) is placed into the NAS. The FA located in the NAS periodically sends advertisements with challenge packets, and all mobile stations register via the FA. The challenge is a piece of data used to verify if the user device has knowledge of the secret (e.g., a password) without sending it explicitly via a communication link. The architecture is able to process two horizontal roaming scenarios:

The current IEEE802.11 device connects to the network via the NAS: The network can provide IP mobility, but roaming is not seamless. When a mobile user requests Mobile IP services by sending Mobile IP Registration, the NAS blocks the Registration until the mobile user has been authenticated via the AAA architecture. The NAS extracts a Mobile-AAA Authentication extension from the Registration Request message. Once the mobile user is authenticated



■ **Figure 4.** *Wireless LAN roaming.*

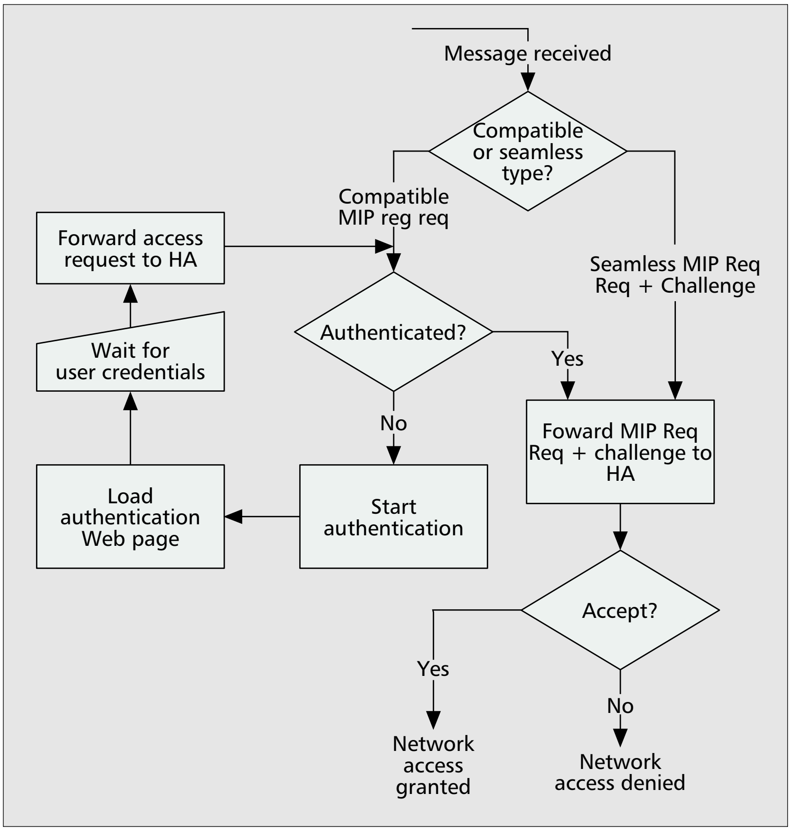
successfully, the normal Mobile IP Registration can be retained.

Seamless roaming: Authentication is completely done by the home agent (HA). The mobile station is required to support Mobile IP Challenge/Response extensions with a Mobile-AAA authentication extension so that the user credential can be processed by the program automatically.

In the following we focus on developing efficient signaling process for the two roaming scenarios. The design shares as many common signaling messages as possible. In order to have further integration with 3G cellular networks, the signaling process should also be able to share with the AAA signaling process for 3G networks. Based on the architecture in Fig. 2, Fig. 5 illustrates the internal design of an NAS/FA. It has two modes: one for compatibility of current wireless LAN deployment, the other to better serve in seamless wireless LAN roaming.

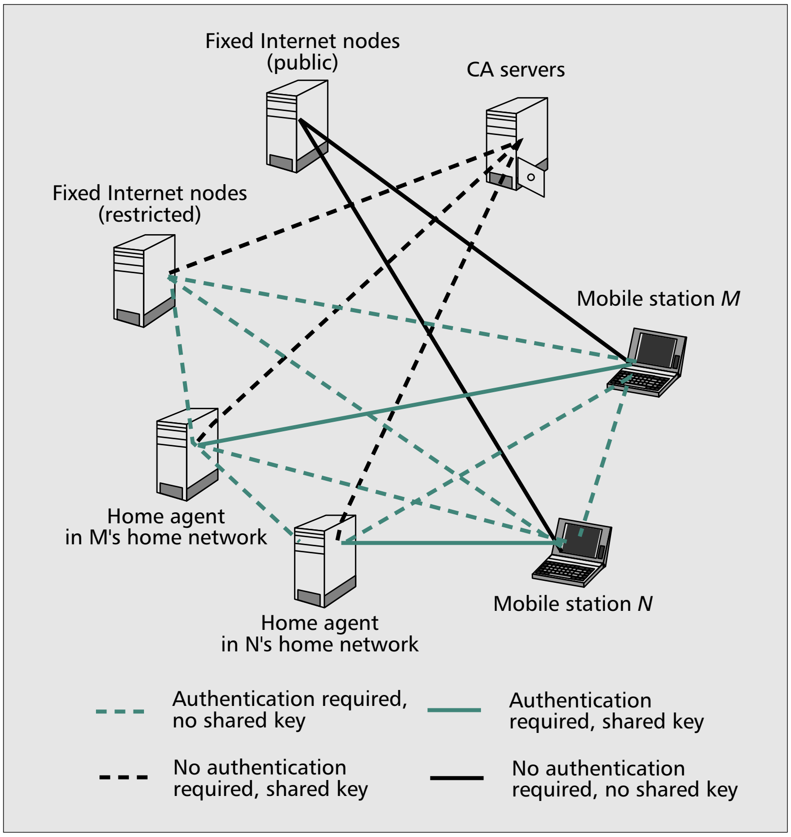
In the compatible mode, when a mobile station registers it may use its home address or the mobile station NAI to identify itself in its Registration Request. A mobile station associates itself with an access point and starts sending IP packets, such as Mobile IP requests, to its HA via an FA that relays the Registration Request. After the HA authenticates this request and sends a reply via the same FA, the HA and FA both update their bindings. Sometimes an FA forces all its serving mobile stations to register through it. If a mobile station does not send the user credentials, including NAI and password, along with the Mobile IP request, the user will be redirected to a login page. By extracting the domain portion of NAI, the authentication request will be forwarded to the AAA server of the WISP. After successful authentication, the Mobile IP request is forwarded to the HA of the mobile station and the Mobile IP registration is completed.

In seamless roaming mode, a mobile station associates with the access point and responds to a Mobile IP FA Advertisement packet with a Challenge, and sends the Mobile IP Registration Request with the NAI and Challenge. The user credentials are included in the Mobile IP request. When the FA receives the reply from the mobile station, it realizes that the mobile station can do seamless roaming. It encapsulates the request in the AMR and forwards it to the AAAH and HA. After the HA processes this request, it sends a HAA containing Mobile IP Registration Reply. The AAAH and AAAL forward the encapsulated Mobile IP Registration Request to the FA in the AMA packets. The FA then sends a Mobile IP Registration Reply.


Message received
Compatible or seamless type?
Compatible MIP reg req
Seamless MIP Req Req + Challenge
Forward access request to HA
Wait for user credentials
Authenticated?
Yes
No
Foward MIP Req Req + challenge to HA
Load authentication Web page
Start authentication
Accept?
Yes
No
Network access granted
Network access denied

■ **Figure 5.** *The flow diagram of the NAS/FA.*

Comparing signaling processes of the two methods, one can see that the processes are designed to be quite similar, such as the signaling messages and the signal path. So some components in the network do not need to differentiate the message type for each mode. Only one signaling processing mechanism need be designed. The FA's own local clients still can


Fixed Internet nodes (public)
CA servers
Fixed Internet nodes (restricted)
Mobile station M
Home agent in M's home network
Home agent in N's home network
Mobile station N
Authentication required, no shared key
Authentication required, shared key
No authentication required, shared key
No authentication required, no shared key

■ **Figure 6.** *Authentication for Internet applications.*

access the hot spot as they can use AAAF to authenticate themselves.

Mobile IP Handoff Performance Improvement

In order to roam between a wireless LAN and a cellular network, the mobile station should be equipped with corresponding network access interfaces. The data packets from the corresponding server are routed to the mobile station through its HA. When the mobile station roams to the foreign network, the two network access cards are assigned a temporary care-of address by the FA.

The switching of the two interfaces can be considered a care-of address change in Mobile IP. When the mobile station decides to switch the interface, it informs the HA by updating its current care-of address to the IP address of the other network access interface. The HA redirects the data flow to the new IP address. This method ensures that the process of network access interface switchover is dealt with using the switching process in Mobile IP.

For typical data applications such as Web surfing, it is not necessary to use real-time seamless handoff as cellular telephony. A gap of a few seconds while a connection is being rerouted will cause no great harm. However, with the growth of real-time Internet applications like voice or streaming video, Mobile IP handoff latency and packet loss performance have become more and more critical. If we want to provide high-quality applications in a wireless LAN environment, the key issue is to support efficient and seamless network handoff. When a mobile station moves from the coverage of one access point to another, it reassociates with a new AP. This is called a layer 2 handoff. On the other hand, a Mobile IP handoff (layer 3) is the process that takes place when changing FAs. The latency generated by both layer 2 and Mobile IP handoffs should be reduced.

In order to reduce the latency of Mobile IP handoff in a wireless LAN, link layer update frames and movement notification packets can be used to assist Mobile IP handoff. A MAC bridge or data tunnel is established between the new FA and old FA servers to improve the latency of Mobile IP handoff in the wireless LAN environment. The pre-registration and authentication data can be sent to the mobile station before it moves, and/or the data packets that arrive at the old FA during movement can be sent to the mobile station via the new FA. Additional flow control should be taken in the handover period, because the connection speed of the old and new access point/base station could be quite different if the mobile station performs handoff between IEEE 802.11 and cellular networks. If the data source is not informed in a timely way, data may block the channel if the device is moving from high-speed to low-speed connection, or the user cannot get better quality of service otherwise. Therefore, effective congestion control is very important, especially for media streaming service that uses the protocol without an inherent congestion mechanism. Measures should also be taken to ensure that the pre-authentication data transfer between the two FAs is private and unaltered. So the two FAs authenticate each other via a CA server using the scheme proposed in the next section, and a temporary session key can be negotiated to encrypt the pre-authentication data.

Wireless Transmission Privacy

Although the architecture proposed earlier prevents an unauthorized user from using the service, the wireless transmission is still kept open. Using built-in WEP encryption cannot guarantee data transmission privacy in a public hot spot, since a WEP key is unique for each access point and there is no privacy among the mobile stations associated with an access point. A separate authentication and key negotiation mechanism is required to keep wireless transmission private.

In this section we propose a scheme that operates at the application layer to avoid any hardware or low-level protocol modification, and the authentication messages are carried in the payload of data packets used in Mobile IP networks. User location updates are transparent to the scheme since user mobility is handled in the network layer. It is an end-to-end solution, so it secures not only the wireless data link in hot spots, but also the entire data path. The FA just relays the authentication message between the mobile station and its home network, and vice versa.

Analysis of Authentication for Current Internet Applications

Various types of authentication with different security requirements, which may occur in applications running on a mobile station, are shown in Fig. 6. For example, a fixed public Internet site may be visited without authentication, while mobile user *M*'s home network may only be accessed by *M*, and there is already a shared key between *M* and its home network. For clarity, these situations are sorted into three categories:

- *Authenticating parties share a secret key*: authentication between a mobile station and its HA. The secret key can be stored in either the mobile station or its Subscriber Identity Module (SIM) card.
- *Authenticating parties do not share a secret key*: authentication between two mobile stations or a mobile station and a fixed Internet server, and so on. Since the two parties have no common secret key to share, more public key algorithm computations are involved.
- *Visit the Internet public resource*: Since the resource is open to the public, no authentication is needed.

Thus, parties authenticated with mobile stations are divided into two categories from a mobile station's point of view — home network and any authentication parties other than the home network — in order to simplify the protocol and future implementation on the mobile station side. In cases other than authentication between a mobile station and its home network, the home network performs the major authentication job and then passes the authentication result to the mobile station.

Characteristics of the Proposed Authentication and Key Negotiation Scheme

In Fig. 2, the fixed networks are identified by the information issued by the CA server. Identity verification is carried out using the public key encryption and digital signature algorithms. Since CA servers are responsible for large amounts of certificate issuing, the task for CA servers in the proposed scheme is simple, no more than looking up the database and sending the necessary information, such as the public key message, to the corresponding receiver. A mobile station never contacts the CA server in the scheme, since it is not practical for a CA server to record the certificate information of all mobile stations because of their enormous population. The certificate of each mobile station is stored in its home network. Thus, each home network server can be considered a CA server of its mobile stations.

A CA server works as a bridge connecting the domain servers, such as HAs and fixed servers. A fixed server can be considered an HA without clients. The proposed scheme puts the corresponding daemon programs into each node and is designed with the following considerations to compensate for salient features or limitations in both hardware and transmission environments:

- The scheme should be intelligent. The design should enable the scheme to adapt to various application scenarios. The adaptation should be mainly implemented in wireline servers.
- The number of different types of message for mobile stations should be limited compared to the home network. Such a design could make the mobile station lighter.
- It is desirable to move much of the computation to the corresponding HAs who have more computation power, high speed, and reliable wired network connections. At the mobile station, intensive computations are limited. Only critical data such as secrets and their hash values are encrypted using a public key algorithm. The public key encryption and digital signature algorithms are not used simultaneously in one message.
- The length of messages will be collected for protocol latency evaluation. According to the network structure, the major presence of latency should be in the wireless part, especially when the client is connected to a cellular network. The design goal is that the time taken to transmit all messages in the slowest connection method be less than 3 s.

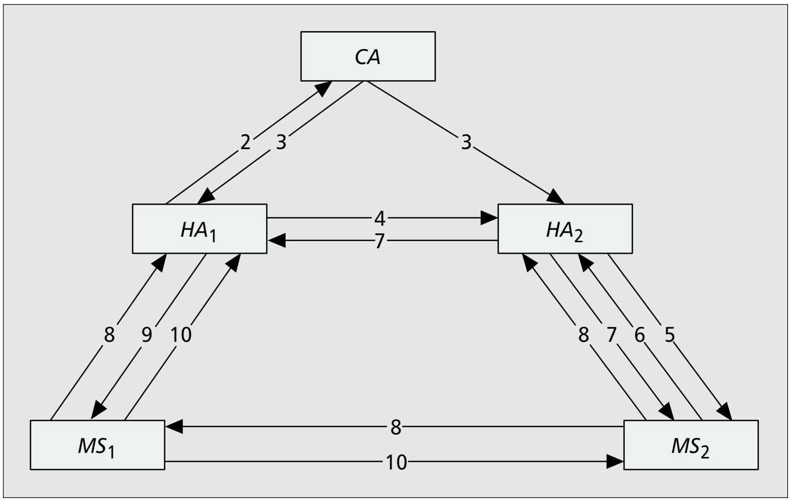


Figure 7. *Authentication and key negotiation protocol between two mobile stations belonging to different home networks.*

A Wireless Transmission Privacy Mechanism

The scheme serves as an authentication service provider to other wireless Internet applications. Before an Internet application begins to send data, the scheme does the authentication first and negotiates a shared key of which the foreign network has no knowledge. At the sender side, all the upcoming data generated by the Internet application with security requirements are encrypted by this shared key. The encrypted or wrapped data are then sent to other data processing blocks. For example, they can be further encrypted by the key acquired by the registration process. At the receiver side, the process is reversed. Thus, a foreign network cannot get plain text even if it holds a key generated during the registration process, and the wireless transmission part is also secured.

There are a few authentication scenarios. We assume that mobile station 1 (MS_1) wants to establish a connection with mobile station 2

Security analysis here includes data privacy, the built-in feature for dealing with certain security compromises. The device-related information is divided into two categories. Device ID and public key belong to normal sensitive data, which means they will not do harm to the system even if they are leaked.

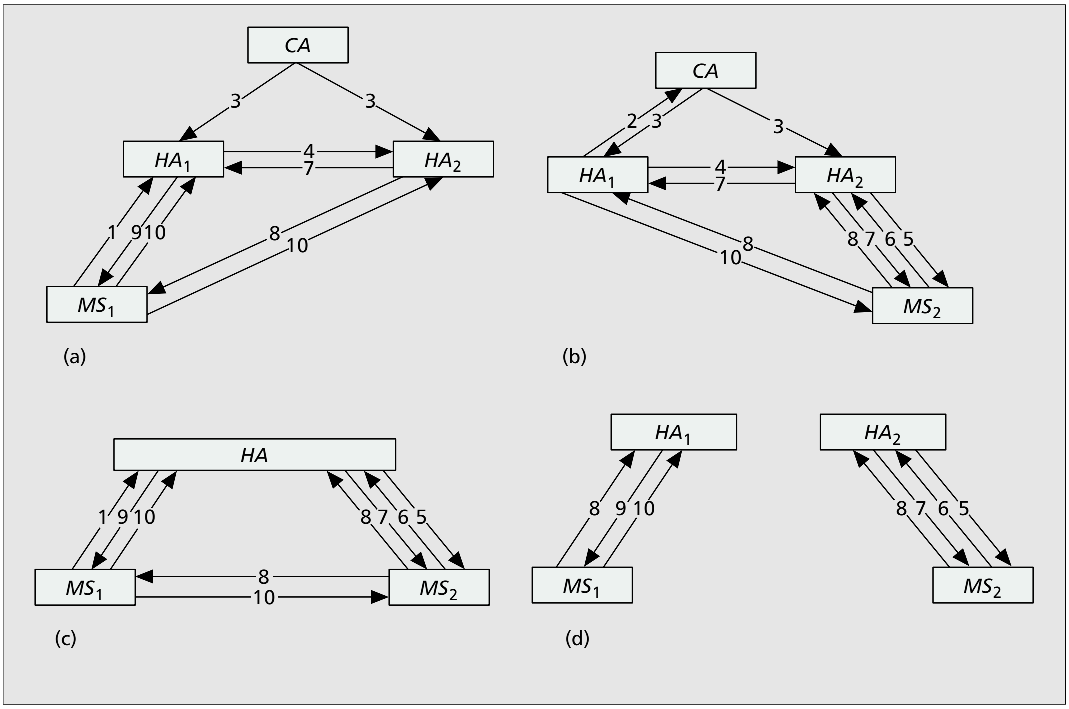


Figure 8. *Scheme variation in various authentication scenarios: a) a mobile station to a fixed Internet server; b) a fixed Internet server to a mobile station; c) a mobile station to another within the same home network; d) a mobile station to a home agent and a home agent to a mobile station.*

(MS_2) via wireless Internet. MS_1 and MS_2 belong to different home networks and have no shared key. This is the most complicated scenario, sharing no secret key. Other cases are considered its subsets. The mechanism works this way and is shown in Fig. 7. The numbers in the figure represent the sequence of steps.

1. MS_1 finds MS_2's home address and creates a nonce with the corresponding hash value. The nonce is used to verify the identity of MS_2. The nonce and its hash value are encrypted by HA_1's public key. MS_1 sends the authentication request to HA_1. The whole message is encrypted by the shared secret key of MS_1 and HA_1.

2. HA_1 decrypts the message from MS_1; HA_1 realizes that MS_1 intends to authenticate with a third party. HA_1 is able to find MS_2's HA, HA_2, from the IP of MS_2. In order to discover if HA_2 is legal, HA_1 contacts *CA* for some information on HA_2, such as the public key of HA_2.

3. *CA* decrypts the message from HA_1 and verifies IDHA_1. *CA* searches its database, and finds the public keys of both HA_1 and HA_2 and the device ID of HA_2. *CA* attaches its digital signature and transmits HA_1's public key and device ID to HA_2 and HA_2's to HA_1.

4. HA_1 decrypts the message from *CA*, and gets the public key and device ID of HA_2. HA_1 stores the pub_{HA2} and ID_{HA2} pair. HA_1 generates the temporary session key. HA_1 forwards the authentication request and temporary session key to HA_2. The key is encrypted by HA_2's public key. So far, there are two messages in step 3 and 4 sent to HA_2.

5. HA_2 will buffer the latter if the latter comes before the former. By receiving message in step 4, HA_2 can get the device ID, IP, and public key of HA_1. HA_2 can also get the device ID and public key of the authentication originator, MS_1 in this case. So HA_2 initiates the authentication with MS_2, because it is not secure to send the identification information before HA_2 realizes it is talking with MS_2. HA_2 temporarily stores the session key and starts authentication with MS_2.

6. Similar to step 1, MS_2 starts authentication with HA_2 using a nonce and its hash value pair.

7. After HA_2 verifies the identity of MS_2, HA_2 sends MS_1's identify information and the session key to MS_2. HA_2 also sends MS_2's identity information to HA_1.

8. MS_2 sends a confirmation to HA_2 and contacts MS_1 by using a new nonce and its hash value encrypted by the session key.

9. HA_1 sends MS_2's identity information and the session key to MS_1.

10. MS_1 sends a confirmation message to HA_1 and replies to MS_2 by sending the hash value of the new nonce.

11. MS_2 verifies the received message from MS_1.

The scheme is also adaptive to other scenarios. For example, if a mobile station wants to authenticate with a fixed server, we consider HA_2 and MS_2 as one unit, and steps 5, 6, 7, and 8 are not necessary. The extended scenarios are shown in Fig. 8.

Security Analysis

Security analysis here includes data privacy, a built-in feature for dealing with certain security compromises. Device-related information is divided into two categories. Device ID and public key belong to normal sensitive data, which means they will not do harm to the system even if they are leaked. Shared secret key and private key belong to permanent critical information that must not be compromised. The nonce and session key generated in the scheme belong to short-term critical information that can affect the ongoing session in which an attacker can discover communication contents. However, if the permanent critical information is still good, short-term critical information is safe because it is encrypted by the permanent critical information.

In the authentication scheme the exchanged message, except for digital signature in the authentication process, are all encrypted by a shared secret key between the HA and the client, or the session key using a symmetric encryption algorithm. More important information like the session key is further encrypted by a public key algorithm and capsulated by symmetric encryption. The authentication message is no different from the normal payload of a TCP packet, so the foreign network can just route it to the destination. The foreign network and other intruders are not able to discover the information inside because they do not have the shared key; and they must have both corresponding shared key and matched private key to get the session key.

Figure 9 shows the distribution of sensitive data after authentication is completed. Normal sensitive information is spread to trusted sites and devices only. The scheme ensures that no sensitive information is released before the information receiver is identified. No permanent critical information is sent in any form during the authentication. Temporary critical data are spread to trusted sites only.

The scheme should be designed to resist certain security compromises. In our authentication scheme, illegal possession of someone's device ID, home IP address, and public key will do virtually no harm to the system. The home network always uses the corresponding shared secret key to process messages according to the carried home IP address. It is the shared secret key and private key that build up the real or final authentication process.

Comparing the shared secret key and private key, a shared secret key is more likely to be compromised because at least two parties, the home network and mobile station, have a copy of the key. Only one copy exists in the mobile station for the private key case. A private key is never given out because it is not necessary due to the nature of public key algorithms. In our scheme, for example, if the shared secret key is leaked, the intruder can get only the device ID, IP address, and public key, which belong to normal sensitive information and do virtually no harm to the system, because the device ID is used for quick identification, and the public key itself is originally open to the public. But it could be harmful if this key is also used on other occasions such as mobile station registration, since the registration process should be done very quickly to avoid the connection being dropped, so there is no time to execute additional time-consuming public key algorithms.

If a shared secret key is leaked and an intruder tries to use it without a proper private key, the system can detect the compromise of the shared secret, because in our authentication scheme, each entity involved is required to return a hash value that can only be achieved by its private key or attach a digital signature to the message. Once the system detects this flaw, it indicates that the common secret key is leaked and the user should be warned immediately. The system cannot detect the private key flaw though, because without a proper shared secret key, the system cannot look into the message. So only when the shared secret and corresponding private keys are broken simultaneously can the intruder access the network illegally. The system is able to detect a security compromise of the shared secret key, but not of the private key. Fortunately, the private key is unlikely to be leaked due to the nature of public key algorithms.

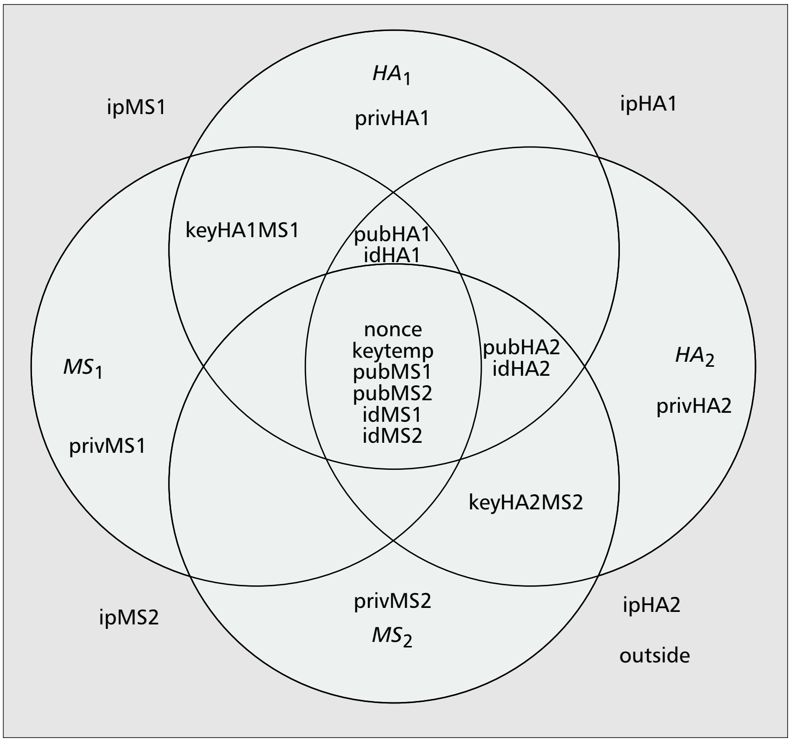
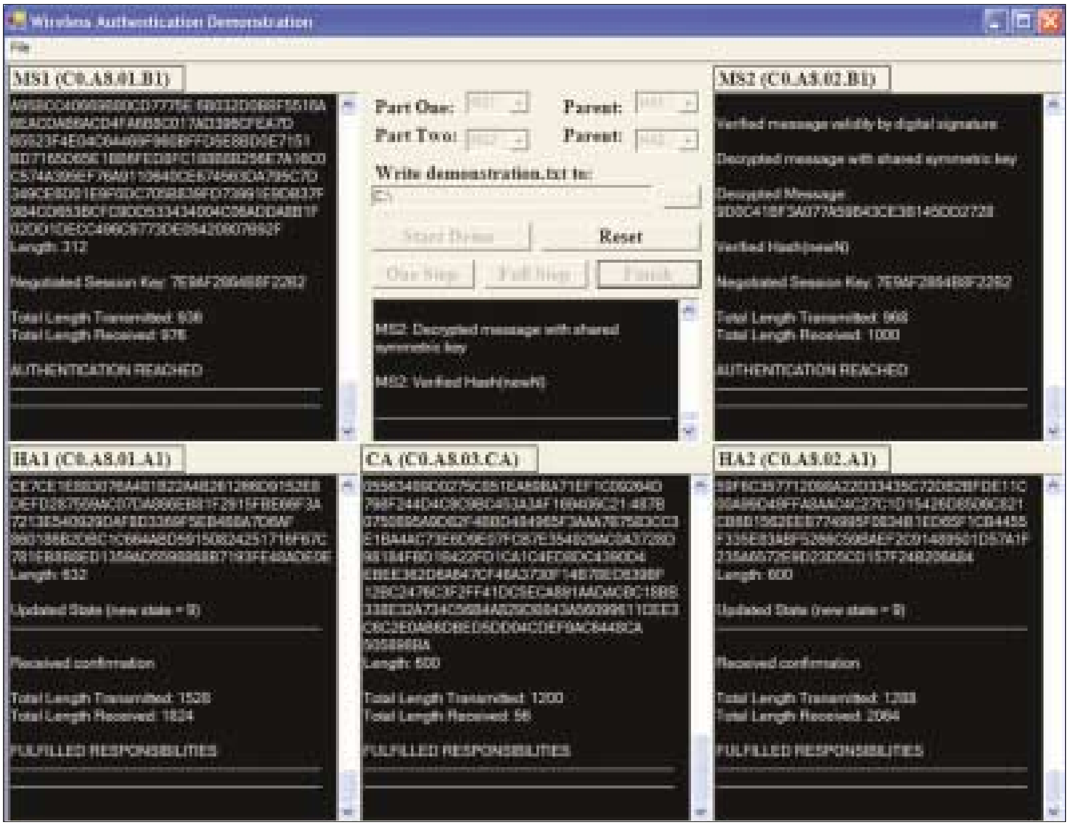


Figure 9. *Secret and identification information control.*

The scheme is also designed to resist replay attack. Every authentication session between an HA and a mobile station, or two mobile stations or two HAs is completed by using fresh nonces and fresh session key, so replay attack has no effect on it. Since the information exchanged between an HA and a CA server represents facts on the clients' identifications and public keys, simply replaying this message does no harm to the system unless the intruder can change the payload and the corresponding digital signature, which is very hard unless the intruder can get the CA's private signature.

In order to totally clone a component (mobile station, home network server, CA server), the malicious user at least needs a proper home IP address, device ID, shared secret key, and private key to satisfy the authentication scheme completely, or it will be rejected at the corresponding step where the item is checked.

In order to totally clone a component (mobile station, home network server, CA server), the malicious user at least needs a proper home IP address, device ID, shared secret key and private key to satisfy the authentication scheme completely, or it will be rejected at the corresponding step where the item is checked.



```
A9SBCC40989880CD7775E 68032D088F5516A
85ACDA8BACD4FA6B8C017A0398CFEA7D
65523F4E04C64489F86BFFD5E88D9E7151
8D7165D65E 1888FED8FC1888BB256E7A18C0
C574A399EF76A011084DCE674563DA795C7D
349CF8D01E9F0DC705B639FD73991E9D837F
984C0853BCFC8DD53343404C08ADDA8B1F
02D01DECC496C9773DE05420807892F
Length: 312

Negotiated Session Key: 7E9AF2894B8F2262

Total Length Transmitted: 936
Total Length Received: 976

AUTHENTICATION REACHED
```

```
MS2: Decrypted message with shared
symmetric key

MS2: Verified Hash(newN)
```

```
Verified message validity by digital signature

Decrypted message with shared symmetric key

Decrypted Message
9D0C418F3A077A59B43CE38145DD2728

Verified Hash(newN)

Negotiated Session Key: 7E9AF2894B8F2262

Total Length Transmitted: 968
Total Length Received: 1000

AUTHENTICATION REACHED
```

```
CE7CE1E8830786A401B22A4826128BD9152E8
C4EFD28759AAC07DA866E881F2915FBE66F3A
7213E5409290DAF8D3366F5EB468A7D6AF
9801868208C1C664A6D5915082425171 6F67C
781EB889ED135AAD559888887193FFE49AD60E
Length: 632

Updated State (new state = 9)

Received confirmation

Total Length Transmitted: 1528
Total Length Received: 1824

FULFILLED RESPONSIBILITIES
```

```
05563489DD0275C851EA86BA71EF1C06264D
798F244D4C9C9BC453A3AF169406C21 487B
0750895A9D62F488D484965F3AAA7675DCCC3
E1BA44C73E6D9E07FC67E354929AC0A3728D
98184F8D18422FD1CA1C4ED8DC4390D4
EBEE382D8A847CF48A3730F14B7BED8398F
128C2476C3F2FF41DC5ECA891AADAC8C18B8
338E32A734C5684A829D6843A56999811DEE3
C8C2E0A86DBED5DDD4CDEF9AC8448CA
505898BA
Length: 600

Total Length Transmitted: 1200
Total Length Received: 56

FULFILLED RESPONSIBILITIES
```

```
59F6C35771 2089A22033435C72D82BFDE11C
00A86C49FFA8AAD4C27C1D15426D8506C821
CB8B1562EEB774695F0B4B1ED85F1C84455
F335E83ABF5266C56BAEF2C91489501D57A1F
235A65726ED23D5CD157F24B208A84
Length: 600

Updated State (new state = 9)

Received confirmation

Total Length Transmitted: 1208
Total Length Received: 2064

FULFILLED RESPONSIBILITIES
```

■ **Figure 10.** *The demo program.*

Authentication and Key Negotiation Demonstration

Figure 10 shows the demonstration program for all the considered scenarios. The demonstration shows the authentication progress, the way the scheme self-adapts to each case, and message lengths sent and received by each node. The demonstration uses RSA as the public key algorithm, DES as the symmetric algorithm, and MD5 as one-way hash functions. Since the proposed scheme is cryptographic-algorithm-independent, other stronger or lighter algorithms can be used to accommodate specific application requirement. The demonstration also shows that the total amount of data for the mobile node is less than 2 kbytes. If the slowest network connection speed is 14.4 kb/s in the cellular network with overhead of the transmission considered, the data transmission can be finished in less than 3 s.

Summary

In this article a network architecture and a set of signaling mechanisms are developed to support current available wireless LAN hot spot roaming. The proposed architecture offers a smooth transition of wireless LAN hot spots from non-roaming-supported to seamless-roaming-supported, so previous investment is protected. A fast network switchover mechanism is available to improve the performance of streaming applications. Meanwhile, wireless transmission security is carefully considered. An application layer authentication and key negotiation scheme is developed to keep air transmission secure. The results can enable wireless LAN roaming, enhance wireless communications, and speed up deployment of public wireless LAN applications.

Acknowledgment

This work has been supported by a Natural Science and Engineering Council (NSERC) Postgraduate Scholarship and a research grant from Bell University Laboratories (BUL), Canada. We would like thank Matthew Cruickshank for his help in the demonstration programming.

References

[1] C. S. Loredo and S. W. deGrimaldo, "Wireless LANs: Global Trends in the Workplace and Public Domain," The Strategies Group, 2002.

[2] A. T. Campbell *et al.*, "IP Micro-Mobility Protocols," *ACM SIGMOBILE Mobile Comp. and Commun. Rev.*, vol. 4, Oct. 2001, pp. 45–54.

[3] C. Perkins, "IP Mobility Support," RFC 2002, Oct. 1996.

[4] J. R. Walker, "Unsafe at Any Key Size: An Analysis of the WEP Encapsulation," IEEE doc. 802.11-00/362, Oct. 2000.

[5] W. A. Arbaugh, "An Inductive Chosen Plaintext Attack Against WEP/WEP2," IEEE doc. 802.11-01/230, May 2001.

[6] J. Zhang, "A Secured Registration Protocol for Mobile IP," private commun., Apr. 1999.

[7] Sufatrio and K. Y. Lam, "Mobile IP Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication," *I-SPAN '99*, Fremantle, Australia, 1999, pp. 364–69.

[8] J. S. Stach, E. K. Park, and Z. Su, "An Enhanced Authentication Protocol for Personal Communication Systems," *IEEE Wksp. App.-Specific Software Eng. Tech.*, Dallas, TX, 1999, pp. 128–32.

[9] H. Lin and L. Harn, "Authentication Protocols with Non-repudiation Services in Personal Communication Systems," *IEEE Commun. Lett.*, vol. 3, 1999, pp. 236–38.

[10] U. Carlsen, "Optimal Privacy and Authentication on a Portable Communication System," *Op. Sys. Rev.*, vol. 28, 1994, pp. 16–23.

[11] C. Park *et al.*, "On Key Distribution and Authentication in Mobile Radio Networks," *Proc. Advances in Cryptology-Eurocrypt '93*, Szombathely, Hungary, 1993, pp. 461–65.

[12] M. Tatebayashi and D. B. Newman, "Key Distribution Protocol for Digital Mobile Communication Systems," *Proc. Advances in Cryptology-Crypto '89*, Houthalen, Belgium, 1989, pp. 324–33.

[13] B. Aboda and M. Beadles, "The Network Access Identifier," RFC 2486, Jan. 1999.

[14] P. Calhoun and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4," RFC 2794, Mar. 2000.

[15] E. Shim and R. D. Gitlin, "Reliable and Scalable Mobile IP Regional Registration," Internet draft, <draft-shim-mobileip-reliable-reg-00.txt>, Apr. 2001.

Biographies

Minghui Shi received a B.S. degree in 1996 from Shanghai Jiaotong University, China, and an M.S. degree in 2002 from the University of Waterloo, Ontario, Canada, both in electrical engineering. He is currently working toward a Ph.D. degree at the University of Waterloo. His current research interests include wireless LAN/cellular network integration and network security.

Xuemin (Sherman) Shen [SM] (xshen@bbcr.uwaterloo.ca) received a Ph.D. degree (1990) from Rutgers University, New Jersey, in electrical engineering. From September 1990 to September 1993, he was first with Howard University, Washington, D.C., and then the University of Alberta, Edmonton, Canada. Since October 1993 he has been with the Department of Electrical and Computer Engineering, University of Waterloo, Canada, where he is a professor. His research focuses on mobility and resource management in interconnected wireless/wireline networks, UWB wireless communications, and ad hoc networks. He is a co-author of three books, and has publications on wireless communications and networks, control. and filtering. He serves as Technical Co-Chair, IEEE GLOBECOM '03 Symposium on Next Generation Networks and Internet, and ISPAN 2004; and as an Editor for *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Vehicular Technology*, *DCDIS*, *Wireless Communications and Mobile Computing* (Wiley), and the *International Journal on Computers and Applications*. He has also served as a Guest Editor for *IEEE Journal on Selected Areas in Communications*, *IEEE Communications Magazine*, and *IEEE Wireless Communications*. He received the Premier's Research Excellence Award from the Province of Ontario for demonstrated excellence of scientific and academic contributions in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, for outstanding contributions in teaching, scholarship, and service in 2002. He is a registered Professional Engineer of Ontario, Canada.

Jon W. Mark received a B.A.Sc. degree from the University of Toronto, Ontario, Canada, in 1962, and M.Eng. and Ph.D. degrees from McMaster University, Hamilton, Ontario, in 1968 and 1970, respectively, all in electrical engineering. From 1962 to 1970 he was with Canadian Westinghouse Company, Ltd., Hamilton, where he was an engineer and then a senior engineer. Since 1970 he has been with the Department of Electrical and Computer Engineering, University of Waterloo, where he is currently a Distinguished Professor Emeritus. He was Department Chairman from July 1984 to June 1990. In 1996 he established the Center for Wireless Communications, University of Waterloo, where he is currently serving as its founding director. He previously worked in the areas of adaptive equalization, image coding, and spread-spectrum communications. His current research interests are in broadband communications, wireless communications, and wireless/wireline interworking. He is a former Editor of *IEEE Transactions on Communications*, and a former Member of the Inter-Society Steering Committee of *IEEE/ACM Transactions on Networking*, an Editor of *Wireless Networks*, and an Associate Editor of *Telecommunication Systems*.

The proposed architecture offers the smooth transition of wireless LAN hotspots from non roaming-supported to seamless roaming supported, so that the previous investment is protected.