SECURE USER'S MOBILITY: THE CURRENT SITUATION

M. Komarova, M. Riguidel
ENST, 46 rue Barrault, Paris 13, France
{komarova, riguidel}@enst.fr

Abstract

This paper describes the current situation concerning security in an IP mobile world. It focuses on the problem of inter-domain WLAN roaming. Interoperability and adaptability issues are introduced when a mobile node roams across networks with different settings. The possibility of implementing different authentication schemes for handover operations in terms of quality of service (QoS) and security requirements is analyzed. Factors affecting handover latency and packet loss are presented. There are numerous fast handover solutions for intra-domain roaming. The possibility of their implementation for global roaming is studied.

Keywords: *Wireless LAN, handover, security, mobility management.*

1 Introduction

Low cost and enormous possibilities of IP-based communications have resulted in the growth of their applications. More and more IP devices are becoming mobile and users can have access to different services independent of the location of their point of attachment. These services have different quality of service (QoS) requirements. To meet these requirements, a universal communication approach that enables high quality and secure user communications independent of a visited network and running application should be designed. This paper gives an overview of current requirements and ways of satisfying them in the context of 802.11 technology.

The paper is organized as follows: Section 2 gives an overview of the handover process and describes mobile nodes and network operations at each Network Reference Model layer. Section 3 presents a classification of commonly used mobility management protocols and analyses current security claims, issues and proposed methods of dealing with them.

2 The handover process

Handover (or handoff) is a process that allows a mobile node (MN) continuous access to a multimedia service even while changing the point of attachment.

The structure of IP networks in general is similar. A set of access points (AP) covers an area, which belongs to an Extended Service Set (ESS), managed by a switch or a bridge. Several ESSs form a subnet in which at least one router is present. A number of subnets constitute an administrative domain that borders with others domains via a Network Access Gateway (NAG). In Fig. 1 different handoff types are shown. The most frequent is a Cell or link-layer handoff (scenarios 1, 4), when a MN moves from an Access Point area to a new one within the same subnet. This type of mobility must be transparent for upper layer protocols and applications.

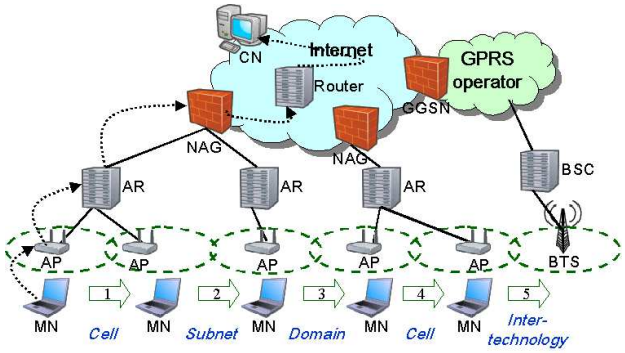

Fig. 1 – Different types of handoff

When a MN chooses an AP in another subnet in the same administrative domain, it executes a Subnet handoff (Fig.1, scenario 2, *macro mobility*). This procedure consists of a cell handoff operation and the acquisition of a new IP address in a visited subnet. A Domain handover (Fig.1 scenario 3, *roaming*) includes subnet changing and Authentication, Authorization and Accounting (AAA) procedures between administrative domains. If there is a need to switch between WLAN and, for example, a cellular network (GSM/GPRS/UMTS), an intra-technology handoff occurs.

Handoff time is the time interval between the last communication packet received (sent) at an old point of attachment and the first communication packet received (sent) at a new one.

A *mobile user* expects to move across networks smoothly without knowledge about their structure, to carry out authentication only at the beginning of a session, not to have to care about protocols and services configurations (they should be self-configurable), to be assured of data protection and to be correctly charged for services used.

A *commercial network* is supposed to serve as wide a range of users as possible, having a low background load.

A *host mobility management protocol* needs to be: independent of underlying wireless and network (IPv6/v4) technology; compatible with other protocols; to be able to support both real-time and non-real-time applications and to work with both TCP ("as is") and UDP/RTP transport.

2.1 Physical layer: hard and soft handoff

Physically handoff duration depends on the type of network card and the number of network interfaces. The latter defines whither a hard or soft handoff can occur. In the case of a hard handoff a MN first loses a connection to a current AP, and then begins to search for a new one, this technology is called "break before make". A soft handoff uses "make before break" technology, when a MN has simultaneous connections to both old and new APs. Soft handoff requires support from visited network entities.

To estimate permissible soft handoff latency two situations were considered: a user with a mobile device walks (at a velocity of 1.39 m/s) and rides in a car (at a velocity of 27.78 m/s) from cell to cell. In both situations the range of the AP used was about 300ft (91.44m) and it was assumed that all APs in a region were placed evenly (width of overlap region is 12.25m). In this way a soft handoff execution will take not more then 8.82 s in the first case and 0.44 s in the second. It is obviously impossible to create a MN managed subnet or domain handoff with high user speed as a condition. The next sections will focus on mobile user operation in 802.11 access networks.

2.2 Link-layer handoff

The figure below summarizes operations executed by a MN in order to change a point of attachment.

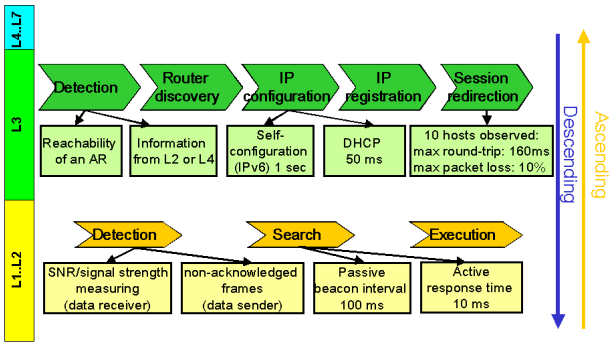

Fig. 2 – Changing of a point of attachment

A MN needs to be connected to an AP to participate in network communications. To be transparent for upper-layer protocols and to minimize packet loss a link-layer handoff should take as little time as possible.

Detection phase: A MN can receive or send data or participate in a bi-directional session. The role of the MN determines the mechanism for the detection phase of a handoff procedure. If the MN acts as a data sender and does not receive acknowledgement for a sent frame, it must decide what takes place: collision, radio signal fading or a handoff. In the case of data receiving the MN listens for an AP's beacon. Another method for handoff detection, faster then the previous, is based on permanent measuring of signal strength or/and signal-noise ratio (SNR).

Search phase: After detection of a requirement to change the AP, the MN begins to look for the most appropriate AP's signal level on different channels (11 channels for USA and 13 for Europe). An 802.11 standard proposes two scanning modes for this: passive, when a MN listens to each channel (default beacon interval is 100 ms), or an active, faster mode, in which a station sends probe requests to each channel (response time is about 10ms) [1].

Execution phase: the MN authenticates itself to an AP chosen at the search phase, sends it a re-association request and waits for a re-association response. The AP and the MN exchange 2 messages without an authentication procedure.

Use of two network interfaces (soft handoff), execution of handoff phases in parallel [1] and improvement of each phase performance separately [2] have been proposed and these methods permit a reduction in link-layer handoff time from 1000 ms to 10 ms.

2.3 Network layer operations

Changing of a point of attachment must not be masked from an IP layer in a case of macromobility. The implementation of subnet handoff detection methods depends on the role of the MN (sender or receiver), and often relies on cross-layer interaction, when a link-layer or an upper-layer protocol informs an IP layer about changing.

After handoff detection an IP address has to be configured. This procedure may be managed either by the MN (IPv6) or by visited network entities (with DHCP). These two approaches for address acquisition are compared in Table 1.

TABLE 1
ADDRESS CONFIGURATION WITH IPV6 AND DHCP

Address self-configuration (IPv6)	**Address configuration using DHCP**
Time to configure address:	
$T_{add}=T_{prefAdv}+T_{addrConf}+T_{DAD}$ (1) if router advertisements are solicit: $T_{prefAdv}=T_{rtAdv}-T_{rtSol}$ (2) when it is periodic: $T_{prefAdv}=T_{AdvInt}/2$ (3)	$T_{add}=T_{DHCPaddr\,Req}+T_{DHCPaddr\,Resp}$ (4)
Information about network entities gathered in one step:	
IP address	IP address; Network mask; Default Gateway address; DNS server address; Net BIOS Name server address; lease period in hours; IP address of DHCP server.
Operations:	
router discovering (wait time varies between 0.5 and 3 sec); address configuration; duplicate address detection (DAD, takes about 1 sec)	DHCP discovery (2 messages, default waiting time for a response is 50 ms); address acquisition (2 messages) delay is represented by a transmission delay

When the MN offers some service or participates in communications, it must be reachable from an external world. Registration of a MN's new address is made with

entities like Home agent for MIP [3] or Registrar/Location server for SIP [3]. The MN should inform the CN about its IP address changing. A message often reaches the CN after a significant delay. If there are packet losses on the link, the wait time for session redirection increases. To determine an average delay communication with ten hosts was observed. The maximum round-trip time was 160 ms and the maximum packet loss was 10%, so session redirection may take up to ~360 ms. This value is not permissible for a real-time application running while handoff is executing.

When a subnet handoff takes place without an administrative domain changing, there is no need to redirect a session or to rewrite registration information. Most of networks use NAT/NAPT devices, therefore a MN changes only a *local IP address*.

2.4 Transport layer requirements

The task of transport layer protocols is to retransmit dropped information on the sender side and to recognize duplicate packets and restore the right order of packets on the receiver side. For the classical realization of TCP it is impossible to continue a session when a socket is changed because of a new IP address. To solve this problem alternative protocols based on TCP have been proposed. But these protocols are not widespread, and a CN may not support non-standard realization of TCP. So it is preferable to keep the TCP connection "as is".

Handoff duration is limited by a timeout after which a connection will be killed. This restriction does not play a significant role, because the time to wait to recover a TCP packet is 100 sec according to RFC 1122.

2.5 Application layer requirements

Restrictions to a handover latency depend on a type of application run at a mobile terminal.

Non-real-time applications: nomadic users want access to *Web* sites or *e-mail* services. .

Real-time applications present different restrictions for packet loss and latency. To avoid buffer size and jitter changing, real-time applications are run over UDP with additional tools for transmission control (RTP, RCTP) instead of TCP. For *Voice over IP* (VoIP) there is no point in retransmitting lost packets. Generally acceptable limits for single AP networks are: latency less than 50 ms, jitter less than 5 ms, and packet loss rate less than 1% according to the ITU-T G.107 standard. A need for a handover may be detected at the application layer basing on QoS measuring. For VoIP *Mean Opinion Score* (MOS), *Perceptual Evaluation of Speech Quality* (PESQ) or *E-model* can be used to estimate QoS degradation [5].

A *video data stream* is correlated, consisting of three types of frames for MPEG2 coding; stream decoding is impossible without key-frames (I-frames). Long handover latency increases the probability of loosing exactly one I-frame. This type of application presents strong claims concerning delay, packet loss rate and bandwidth.

The MN may use results of some *program execution* taken from a remote host for some calculations. The main problem is that the sending party may not have enough large buffer to store sent data and drop packets get lost.

3 Mobility management and Security

3.1 Mobility management approaches

The aim of mobility management is to allow a MN to adapt itself to different visited networks while keeping a desired level of QoS.

Public WLANS (hotspots) and enterprise networks present two different types of visited environment. Each user must subscribe to at least one *service/identity provider*, which is responsible for the subscriber's billing. Roaming agreements between different providers create an infrastructure that allows a mobile user to gain network access via any *hotspot operator* participating in such agreements. When users move inside an *enterprise network*, it is assumed that they have all the information needed to re-associate with different APs and ARs in the same administrative domain.

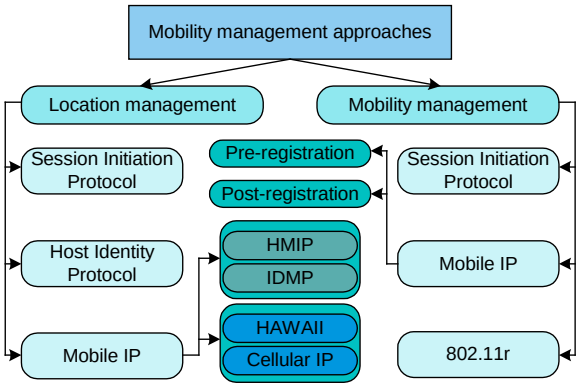

Fig. 3 – Mobility management approaches

Mobility management approaches are classified as location management to support location registration or update and mobility management to keep a connection during changing of a point of attachment (See Fig. 3).

802.11r [6] is designed to support fast handover between 802.11 networks in order to allow VoIP applications running. This protocol is not standardized yet.

Mobile IP (RFC 3775, 3344) allows host mobility over the Internet. This protocol is based on a network infrastructure that includes a Home Agent (HA) in a home network and a Foreign Agent (FA), which must be present in a visited network. The protocol supports mobility management by registering with a FA and location management by address binding at the HA and the CN. The soft handoff emulation is realized by triangular routing. It provides high reliability (using multiple home

agents) and a security layer (protection of signaling, authentication and communication with IPSec), but address binding and secure tunnel re-establishment take a long time. This approach is not scalable for frequently moving users because of a significant handoff cost.

Collaboration with L2 protocols via special messages (triggers) can improve handoff parameters [7]. *Pre-registration handoff scheme* allows the MN registering with a new FA while being attached to an old FA. Registration begins when a trigger, signaling upcoming change at L2, is received.

With use of a *Post-registration handoff scheme* registration occurs when a L2 handoff is completed. This approach is based on a network-initiated model and supposes a bi-directional edge tunnel establishment.

Several modifications allow use of MIP for micro-mobility management. They reduce the number of messages sent to the home network when the MN changes its location in the same region. When the MN first arrives at a foreign network it must register its Care-of-Address (CoA) with the HA. Two types of intra-domain implementations of MIP are proposed: tunnel-based (HMIP and IDMP) and routing-based (Cellular IP and HAWAII).

Hierarchical Mobile IP (HMIP) [8] and *Intra-domain Mobility Management Protocol* (*IDMP)* [9] introduce a packet redirection mechanism within a domain using hierarchy of mobility agents. *Cellular IP* (*CIP)* and *Handoff-aware wireless access Internet infrastructure (HAWAII)* use a cross-layer approach to create paths to the MN moving between APs.

Host Identity protocol (HIP) [12] proposes a Host Identity (HI) namespace and a protocol layer between the internetworking and transport layers. The protocol supports readdressing and authentication services. Transport-layer associations are bound on HI, which allows host changing an IP address without modification of a transport association. The MN must inform the CN about new address(es), and the CN must verify that the mobile node is reachable at this address. A rendezvous mechanism (for frequently moving hosts) is proposed. This mechanism needs a new infrastructure to be deployed.

Session Initiation Protocol (SIP) [4] is designed for establishing, modifying and terminating multimedia sessions. The SIP infrastructure includes a user client and a user server at a terminal, a SIP proxy, a registrar, location and redirect servers, protocol operation does not depend on wireless and network technology. Its ability to modify sessions is used for location updating and handoff management. For mobility management realization it is assumed that each visited domain has a SIP proxy. A session is redirected by exchange of two messages with the CN and soft handoff is emulated by involving local SIP servers [1]. Use of hierarchical registration schemes can reduce the round-trip time of location updates.

MIP and SIP are commonly used for mobility management, but the first suffers from long operation time and the second is unsecured and it presents a risk of interoperability loss.

3.2 Requirements for security realization

For each handover scenario two closely related aspects are very important: latency and level of security. Authentication of a MN presents a key issue due to its significant contribution to the total handoff delay.

There are some factors that increase a system's vulnerability level:

- ✓ wireless communications are open for eavesdropping and it is natural to consider that a channel in use is always being listened to;
- ✓ the MN visits a foreign network with an unknown security level, so end-to-end security must be supported. Address binding at the CN presents also a significant threat. It is very important to protect a mobility service from theft and false handoff.

Independently of the application running the MN passes through typical states. They are listed in Table 2.

TABLE 2
POTENTIALLY VULNERABLE STATES AND SOLUTIONS TO SECURE THEM

State	Threat	Solution
Session establishment	credentials and keys interception, entity impersonation	encryption of signaling information, strong authentication
Session running	eavesdropping	encryption of communication data
Association with a new AP	AP impersonation	mutual authentication with AP
Router discovery, IP address changing	access router impersonation	mutual authentication with an AR
Session redirection	DoS on the CN, session redirection, session hijacking	authenticating and ciphering of redirection massages
Registration with a home server	credentials, location interception and modification	traffic encryption and integrity protection

When the MN operates in a *Public WLAN*, it must implement a strong security policy. If the MN begins a session in an enterprise network, it is registered there and has several access rights. This type of network has a "physical" access protection (guarded territory, building) and provides security services. The MN should have different sets of security policies that are adaptable to external conditions that change dynamically.

A mobile user requests to be authenticated only at the session establishment and, at the same time, to be assured that each visited network is trustworthy. From the user's point of view, communication data must be at least integrity protected and authentication and billing data must be both confidential and integrity protected. After a handoff occurs, a MN should be sure that it continues to

communicate with the same CN as at the beginning of the session.

A *CN* requires an entity that signals about current session redirection to prove that it is what it claims to be. Protection against DoS attacks also must be guaranteed.

A visited *Network* should identify and authenticate a user that asks the network to grant Internet access; correct account user's activity; recognize malicious behavior in a visitor; dynamically build trust relations with other administrative domains in order to authenticate a visitor and distribute/negotiate encryption keys with users.

A MN trusts only a current AP, AR and AS. The MN and an AP cannot trust each other before common secret verification. They must construct keys based on keying material from an AS. The MN should be registered somewhere on the Internet and have a set of credentials certified by a third party which can prove MN's identity to a visited network. For its part, a trusted server helps to verify if the network is what it claims to be.

Several types of link-layer authentication solutions do not provide mutual authentication and strong key establishment and they should not be used without higher-layer authentication mechanisms. *Open System authentication* [6] provides only mobile station's identification using its MAC address. "*Canned success*" grants network access immediately after request without authentication process. *Wired Equivalent Privacy (WEP)* [6] provides security by information encryption at the physical and data link layers. The resulting security level is lower then in wired LANs due to the vulnerable nature of WLANs.

3.3 IEEE standards for WLAN authentication

802.11i (WPA2) provides mutual authentication, integrity, session keys and confidentiality. It uses the Advanced Encryption Standard (AES) with EAP and 802.1X. The authentication results in fourteen messages being exchanged: eight messages for a mutual authentication and eight messages for key construction.

802.1X provides authentication to devices attached to the network. The authentication is usually done by a third-party authentication server, typically RADIUS, which takes care of the mechanism for per-packet authenticity and integrity between an AP and the AS.

EAP-TLS is the default authentication protocol for the 802.11i framework. It combines EAP authentication and TLS certificate checking. As a result two keys are produced: PMK (Pairwise Master Key) and MK (Master Key). The PMK is shared between the MN, the AS and a current AP. Based on this key, the PTK (Pairwise Transient Key) and GTK (Group Transient Key) are produced by the MN and the AP after four-way and two-way handshakes respectively.

802.11f (Inter Access Point Protocol - IAPP) is designed to exchange context between a current AP and a new one during the handoff process. A RADIUS server distributes communication session keys for APs [6].

3.4 Fast authentication methods

Table 3 summarizes the impact of each phase on total handover latency. It is assumed that all steps except authentication are optimized with relation to latency minimization.

TABLE 3
LATENCY OF EACH HANDOVER PHASE

Phase	Time, ms	%
Detection	3 [1]	0.18
Searching	40 [2]	2.35
Execution	2	0.12
IP address configuration	200	11.73
Session redirection	360	21.11
802.11i authentication	1100 [12]	64.52

802.11i authentication provides a high level of security but accounts for the majority of overall handoff latency. Some methods to reduce layer 2 authentication delay are proposed. Fast handoff methods must not violate the trust relations and secret. For all of the proposed methods the first authentication must be full (non-modified).

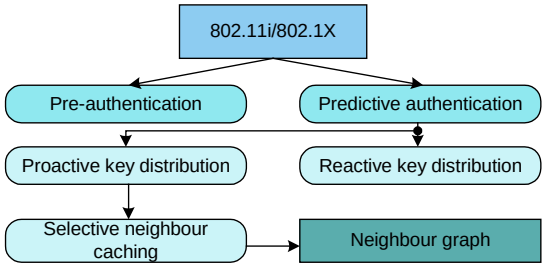

Fig.4 - Fast authentication methods based on 802.11i

Pre-authentication supports one-to-many message exchange. When the MN authenticates an AP, it authenticates to all APs one hop ahead in the subnet. This method introduces new opportunities for DoS attacks and significantly loads an AS [6].

Predictive authentication uses a modified 802.1X key distribution protocol [13]. The significant network load can be reduced by choosing a *Fast Handoff Region (FHR),* the set of APs that are most frequently visited by the MN. A FHR is commonly described with Neighbor Graph (NG) [14], which is used to determine the candidate set of APs with which the MN could potentially associate. This dynamic data structure can be maintained in a distributed manner among APs or in a centralized manner at an AS.

Proactive key distribution [14] enables a reduction in handoff latency and the use of a mobile station's computational power by pre-distributing key material ahead of the MN. The proactive method requires changing at the client, APs and the AS. Instead of a four-way handshake a two-way handshake is used after key distribution: the first message is sent by the MN and the

second is sent if an AP has the correct key.

Reactive method for key distribution, unlike Proactive key distribution, does not require changes at an AP. When an AP sends an EAP Identity Request to a client, it responds with a PMK identifier, the AP asks an AS for a corresponding key (that results in two messages), it sends an EAP Success message and a four-way handshake is performed. The old PMK must be immediately deleted and a new one generated.

As proactive key distribution may cause significant signaling overhead, *selective neighbor caching* is proposed to decrease the number of candidate APs [15]. The method selects a set of adjacent APs based on some threshold value that presents a probability of visiting each AP by a concrete MN. A current AP sends a MN's context only to the selected neighbors with neighbor weights higher or equal to a predefined threshold value. The threshold is determined by a minimization of the signaling cost of transferring context to neighboring APs.

Another method to reduce authentication latency proposes the use of 802.11f protocol for *secure context transfer* [6, 13]. IAPP is not designed for security purposes but provides a standard set of messages, which can contain different information.

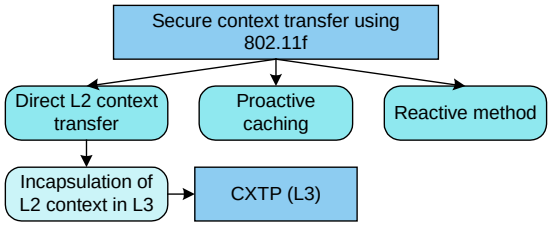

Fig.5 – Fast authentication based on a context transfer

The Reactive method allows the MN to establish a trust relationship with a new AP via a relationship with an old AP. Instead of the keys used by an old AP for encryption a result of some function of these keys is distributed.

Proactive caching enables reduction of the time needed for this transaction. When a MN re-associates to an AP, the latter looks for a corresponding entry in its cache. If such an entry exists and has not expired, an AP sends a re-association response, otherwise it asks for information from the old AP.

Direct L2 context transfer for inter-ESS handover requires a roaming server, roaming agreements and NAT traversal mechanism. This solution can be implemented easily if the AP (or AR) has a public IP address.

Encapsulation of L2 context in L3 context presents an integration of Context Transfer Protocol (CXTP) [16], using the Seamoby working group, and IAPP [13].

All proposed methods allow keeping a high security level but they require lengthy observation, logging and analyzing of MNs' behavior. Secondly, they increase network load. These factors restrict the possibility of its implementation to office/enterprise networks, where there is a constant set of users with stable mobility patterns. Networks, open to public access, cannot grant the required amount of computational resources and traffic to visitors. Extensions of fast L2 authentication methods are proposed for inter-domain handover, but all of them require roaming agreements, infrastructure knowledge sharing between different domains and additional network entities with specific functionality.

3.5 Hotspot authentication methods

Hotspot authentication methods use principles that differ from enterprise network authentication methods: each user can connect to a network, but only an identified one is granted by an external network access [17].

Authentication process relies on a gateway device performing filtering of IP traffic. User enters his credentials on a portal page run at a gateway and protected by Https, and the gateway uses the RADIUS protocol to communicate with a user's service provider. In this case there is no means to secure communication provided: all non-authentication data is transmitted without protection.

If inter-provider federation exists, *Single Sign On* (SSO) [18] technology allows user to access different domains being authenticated just once may be implemented. This approach is based on cryptographic cookies valid not only at the issuer server but also at its roaming partners.

Liberty Architecture [19] operates at the application layer, using the next architectural components: Web services, Web redirection, Metadata and Schemas. Liberty-based roaming has an advantage of hiding user identity and credentials from visited service provider. The disadvantage of the method is a long time taken by an authentication procedure.

Protocol for Carrying Network Authentication (PANA) [20] is a protocol for a MN's authentication for a first access router. It does not require the presence of initial trust relations with the MN or its home AS. The protocol does not introduce new security methods but uses existing ones.

The main issue of hotspot access is the authentication process, which is either manual or time consuming because of searching and information exchange with external identity providers (up to 2 seconds according to [17]). The absence of mechanisms for establishing dynamic roaming agreements makes roaming between previously unknown domains impossible.

4 Conclusions and future work

In this article we observe steps of a handover process, customer requirements to mobility realization, related issues and possible solutions of them.

A good handover performance may be achieved by optimization of physical, link and network layer protocols

operation, but trust establishment and authentication procedures significantly increase overall latency of a process.

Inter-technology and inter-domain roaming requires interaction with a mobility infrastructure, but the user's terminal must recognize and classify situations and react appropriately. In a visited network security settings of mobile terminal might change and such network, from its part, should be able to implement several security levels to satisfy different user requirements.

We describe current trends of fast authentication protocols development. These protocols try to decrease time taken to prove a user's identity to a network and vice versa, but their implementation requires extending of trust relations and sharing of information between different administrative domains.

Federations, created by public access networks, require homogeneous implementation of authentication on each partner side. This restriction slows down infrastructure deployment for ubiquitous mobility. Our future work will face development of fast authentication methods that enable secure seamless user mobility in an environment with heterogeneous authentication approaches.

References

[1] A.Dutta et al., "Fast-handoff schemes for application layer mobility management", *ACM SIGMOBILE Mobile Computing and Communications Review Volume 7, Issue 1*, 2004

[2] A. Mishra and all, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff process", *CS Tech Report CS-TR-4395*, 2002

[3] D. Johnson, C. Perkins, "Mobility support in IPv6", RFC 3775, June 2004

[4] J. Rosenberg, H. Schulzrinne, "Session Initiation Protocol (SIP)", RFC 3261,. June 2002

[5] ITU standards, *www.itu.int*

[6] http://standards.ieee.org

[7] R.Vidhya, S.Jamadagni, "An IAPP-Mobile IP reference interworking protocol", draft-satish-iapp-mip-00, August 2006

[8] H. Soliman et al., "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," Internet draft, IETF, draft-ietfmipshop-hmipv6-02.txt, June 2004, work in progress.

[9] S.Das et al., "IDMP: An Intra-Domain Mobility Management Protocol for Next Generation Wireless Networks", IEEE Wireless Magazine, October 2002

[10] A. Campbell et al., "Cellular IP," draft-ietf-mobileip-cellularip-00.txt, IETF, January 2000,Work in Progress.

[11] R. Ramjee et al., "IP micro-mobility support using HAWAII," draft-ietf-mobileip-hawaii-01.txt, July 2000, Work in Progress.

[12] R. Moskowitz, "Host Identity Protocol Architecture", draft-ietf-hip-arch-03, August 1, 2005, work in progress.

[13] M.S.Bargh at al, "Fast authentication Methods for handovers between IEEE 802.11 Wireless LANs", *WMASH'04*, October 1, 2004

[14] A.Mishra et al, "Proactive key Distribution Using Neighbor Graphs", *IEEE Wireless communications*, February 2004

[15] S.Pack et al, "A Selective Neighbor Caching Scheme for fast handoff in IEEE 802.11 Wireless Networks", *ACM SIGMOBILE Mobile Computing and Communications Review*, 2005

[16] J.Loughney et al., "Context Transfer Protocol (CXTP)", Request for Comments 4067, July 2005

[17] Y.Matsunaga et al, "Secure Authentication System for Public WLAN Roaming", *WMASH'03*, California, USA, - September 2003

[18] The OpenGroup website, http://www.opengroup.org/

[19] J.Hodges and T.Wason, "Liberty Architecture Overview," Version 1.1. Liberty Alliance Project, January 2003, http://www.projectliberty.org/specs/

[20] M. Parthasarathy, "Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements", RFC4016, March 2005

Biographies

Professor Michel Riguidel is the Chair Department of Computer Science and Networks, at ENST, where he lectures in security and advanced networks. His research is oriented towards security of Information Systems and Networks, Architecture of Communication Systems. He is the Head of the Multidisciplinary Thematic Network in security at CNRS (National Scientific Research Center). He belongs to the Executive Board of RNRT (National Network in Telecommunication Research). In the IST Integrated Project of FP6, he is Key Researcher of the SECOQC Integrated Project (Development of a Global Network for Secure Communication based on Quantum Cryptography), responsible of the Network Architecture. He has several patents in security (firewall, watermarking and protecting CD ROM).

Maryna Komarova is currently a PhD student at the Computer Science and Network department in Graduate National School of Telecommunications (ENST) in France, where she works under guidance of professor Michel Riguidel. She received her M.S. degree in Information Management Systems and Technologies from the Dniepropetrovsk National University in Ukraine in 2004. Her research interests include mobility management and security in wireless next-generation networks.