Fast Solutions for AP-to-AP Handoffs

Wenhui Hu
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
Wenhui.Hu@hut.fi

Dan Forsberg
Nokia Research Center
Dan.Forsberg@nokia.com

Abstract

The handoff between Access Points is mandatory in a wireless network. However, the delay cost by the re-authentication during the handoff process is normally much bigger than mobility management itself. The long delay increases the possibility of packet loss during the handoff process and it is harmful to applications which are sensitive to packet loss. The long delay itself is also deleterious to applications like VoIP. There are approaches to reduce the delay caused by the handoff. To reduce the delay also means to increase the performance of the handoff process. This paper analyzes these existing handoff technologies by scope and the type of authentication, tells how different approaches achieve optimization and also suggests a new approach in discussions section.

KEYWORDS: handoff, performance, Access Point, scope, wireless network, authentication, re-authentication

1 Introduction

The key application of the future mobile network often seems to be interactive and a support for Quality of Service (QoS) is needed. A seamless handoff between Access Points (APs) is often considered to be compulsory in the future mobile network. It provides the foundation to support above features when Mobile Nodes (MNs) move between APs.

Operators are normally very sensitive to security of the handoff process. First, non-authenticated packets bring threats to the wireless network, e.g. the possibility of denial of service (DoS) attacks to servers other than APs. Second, non-authenticated packets also means loss of money to some operators. Finally, the wireless security protocols which are used currently are normally designed to do authentication at every AP, e.g. the wireless LAN security protocols [6] and the Global System for Mobile Communications (GSM) uses the same key for authentication in every base station.

When doing handoffs, some packets may be delayed or even lost because of the handoff delay. The first source of the delay is from mobility management. This cost is mandatory and how to reduce it lies on the design of mobility management protocols. Another tremendous source of the delay is re-authentication. The authentication normally needs the assistance from another server or third party, e.g. Public Key Infrastructure (PKI) or an Authentication, Authorization and Accounting (AAA) server when using symmetric key cryptography or self-managed certificates. The communication between the AP and another server or third party costs too much and leads

to a result that re-authentication might cost much more than mobility management. This type of delay of re-authentication in handoffs is harmful to seamless services in wireless networks. For instance, voice over internet protocol (VoIP) requires the one-way transmission interval must be less than 400 ms while the quality of this service becomes better when the one-way transmission interval is less than 150 ms [26]. But according to measurement data by Mishra et al., the delay of a full-authentication with high latency is approx 800 ms [19]. Obviously, this authentication delay is too long to VoIP application.

There are several approaches which try to improve the performance of handoffs by amending the mobility management protocol or reducing the delay of re-authentication. Some approaches even combine these two together. We believe that the design of these approaches affects the suitable scope of the approaches themselves. In this paper, we compare different approaches around IP layer by following factors: how the performance is improved, and how the suitable scope & the authentication methods are affected. We also introduce one new approach in the discussion section based on our comparison.

In this paper, we focus on AP and handoffs. In some parts such as Mobile IP in section 4.1 , Access Router (AR) is used instead of AP because the original references use AR. In this case, we assume the AR also acts as AP. Similarly in some parts, handover is used instead of handoff because the original references use handover. We assume the handoff and the handover have the same meaning in these cases.

The rest of the paper is organized as follows. Section 2 introduces the relationship between scope and mobility management in handoff process. Section 3 introduces user authentication approaches on MNs. Section 4 analyzes existing approaches. Section 5 gives the results and Section 6 provides a suggestion for best possible approach. Section 7 is conclusion.

2 Scope and level of mobility management

In the handoff process, scope means how big area the solution suits for. On the other hand, mobility management can be divided into macro mobility, micro mobility, and nano mobility according to the scope of mobility area [18]. Therefore, the mobility management level has the same meaning of scope in the handoff process.

2.1 Macro mobility

Macro mobility means moving over a large area. One important characteristic of macro mobility is that the IP addresses of MNs change while moving [18]. One example is vertical handoffs [30] in wireless overlay networks. In vertical handoffs, MNs have multiple interfaces and their IP addresses may change. Macro mobility management may happen between different operators or two parts of big operators. In these situations, handoffs need some kind of agreement between two operators or two parts of a big operator.

When between two operators, optimization in macro mobility management is much more difficult to achieve than in micro mobility management. This is because every operator will not allow storing any secret data as password out of its network [8].

2.2 Micro mobility

Micro mobility means moving over a small area. The IP addresses of MNs do not change while moving, but the current network knows the movement [18]. One example is the movement between different APs without the change of IP address. Micro mobility management happens within one

network. The handoffs are processed in the same network and by the same operator. So the operator can choose different ways to do optimization flexibly.

Micro mobility management happens the most. The optimization will provide a much better service to users.

2.3 Nano mobility

Nano mobility means moving over a very small area. Only part of the current network knows the moving and there is no change for IP addresses of MNs [18]. Nano mobility management happens within a small area of one network. The movement within one AP is an example in which nano mobility management happens. So, re-authentications during handoffs can use the same approach as what the micro mobility management uses. For the view of scope, the nano mobility is like a special case of micro mobility. So in this paper, the micro mobility and nano mobility are considered together.

3 User authentication approaches on mobile nodes

The design of the fast solutions decides which type of authentication can be used by nature. We divide these approaches into three types: password based authentication, certificate based authentication, and intervention needed authentication.

3.1 Password based authentication

In this paper, password based authentication means that the authentication is based on shared password. Shared password is a traditional way to do authentication. The network needs AAA servers to store the passwords and access control data, e.g. RADIUS [27] and Diameter [5]. Every AP in the network needs the same shared password to do authentication for a certain MN. In a non-optimize situation, APs will request authentication result from AAA server on demand. In this situation, the communication between APs and AAA server become one source of re-authentication delay.

When people consider how to optimize the performance, one simple idea is to keep some passwords into the APs to avoid transmission delay. But this has a clear limitation. The operator will not give any symmetric secret data to copartner because "an authenticator MUST NOT share any keying material with another authenticator" [8]. This type of optimizing has a visible boundary – the border of operator.

3.2 Certificate based authentication

In this paper, certificate based authentication means that the authentication is based on certificates which use asymmetric key cryptography. Asymmetric key cryptography is becoming more and more popular these days. In wireless networks, it needs the support from AAA servers or the third party. When doing handoff, the MN should authenticate itself to APs by using its private key, while APs verify the MN by its public key.

In a non-optimize situation, using asymmetric key cryptography will normally cost more than the symmetric key cryptography since APs have to connect the corresponding server to get public keys and the calculation of asymmetric key cryptography is slow. But when doing optimization, the asymmetric key cryptography has one big benefit that its public key is public and it is safe to transfer the public key in a unsecured network. This suits especially for macro mobility level solutions.

3.3 Intervention needed authentication

There are also several authentication approaches which need the intervention of users. Image based authentication [10] and biometric authentication [9] are good samples of these approaches. The limitation of this type of approaches is that they can not be done automatically. This type of approaches do not suit for those approaches which require a full authentication during handoffs.

4 Existing approaches

There exist many approaches to solve the handoff problem. In this section, we focus on introducing those approaches which can reduce the delay caused by handoff processes.

4.1 Mobile IP

Mobile IP is an approach to resolve the mobility management. It has both IP version 4 (MIPv4) [23, 21] and IP version 6 (MIPv6) [11]. MIPv4 has Home Agent (HA) and Foreign Agent (FA) while MIPv6 has only HA. HA and FA are intermediator between MNs and Correspondent Nodes (CN).

The authentication of Mobile IP is based on the infrastructure in which Mobile IP works with AAA servers [7]. This infrastructure suits for any AAA protocol. In addition, registration keys should be created between the MN and the HA or FA to protect the data between them [22].

There are several approaches which try to improve the performance of the Mobile IP.

- **MIPv6 Fast Handover**

  Fast handovers for mobile IPv6 (FMIPv6) [24] improves the performance of MIPv6 by doing Layer 3 handoff steps before Layer 2 handoff steps. There is a tunnel between the new Access Route (nAR) and the old Access Route (oAR). nAR does authentication and creates the IP connections (Layer 3) by the data from oAR via tunnel before the handoff happens in radio (Layer 2). The whole process is described in Figure 1. The only delay is the radio (Layer 2) handoff steps.

  In this approach, the optimization comes from doing re-authentication before the real handoff happens. To choose either password based authentication or certificate based authentication is the same since the layer 3 steps are prior to layer 2 steps and the only delay is from layer 2 steps. Intervention needed authentication does not suit because of the need of the re-authentication in the handoff. In practice, FMIPv6 normally uses password based authentication. This approach is suitable for all the mobility management levels.

- **Hierarchical Mobile IPv6 Mobility Management**

  Hierarchical Mobile IPv6 Mobility Management (HMIPv6) [28] is an extension to Mobile IPv6 and IPv6 Neighbor Discovery. This approach is designed to improve the performance of local mobility by reducing the amount of signaling among the MN, CN, and HA. Mobility Anchor Point (MAP) is added. In handoffs, the MN sends only one Binding Update (BU) to the local MAP rather than the HA and CNs to improve the performance is improved. For example, in Figure 2, when MN moves, it sends BU only to the local MAP – MAP3.

  HMIPv6 gets the optimization by altering the mobility management protocol. HMIPv6 uses password based authentication. Certificate based authentication does not suit because of its slow calculation. Intervention needed authentication does not suit because re-authentication in handoffs needs human intervention. HMIPv6 improves the performance especially in micro mobility and nano mobility level since only MAP needs to be informed in these cases. In

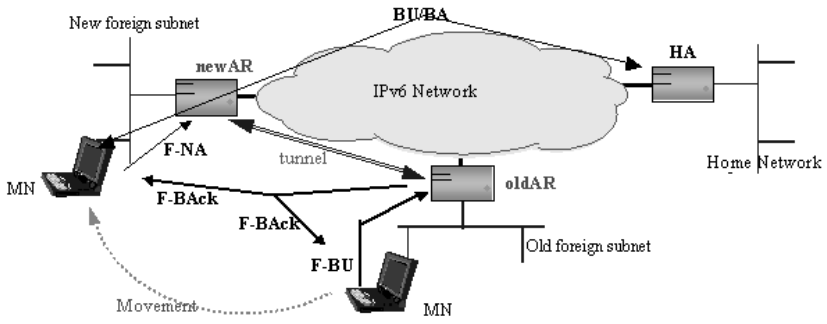

Figure 1: Fast handovers for mobile IPv6 [3]

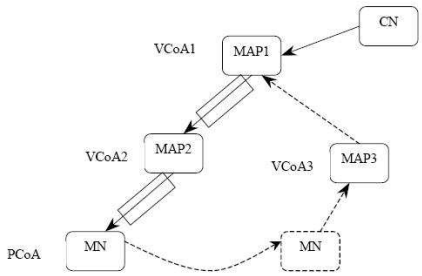

Figure 2: Handoffs in HMIPv6 [29]

macro mobility level, HMIPv6 works without optimization because APs must communicate with AAA server after IP address of MNs changes.

- **Fast handover in Hierarchical Mobile IPv6**

  Fast handover in Hierarchical Mobile IPv6 (F-HMIPv6) [12] aims to combine ideas from both the FMIPv6 and the HMIPv6 together. Simple combination will incur the triangle routing as shown in Figure 3. The main idea of F-HMIPv6 is to use MAP to replace previous Access Router (pAR) in handoff processes. The result is an effective signaling flow as Figure 4.

  F-HMIPv6 reduces both mobility management delay and re-authentication delay. In the case of micro mobility and nano mobility, the performance of handoffs is increased from both sending only one packet to MAP like HMIPv6 and to do layer 3 steps before layer 2 steps like FMIPv6. In the case of macro mobility, the performance is still increased, but only from doing the layer 3 steps first. F-HMIPv6 uses password based authentication. But certificate based authentication also suits since layer 3 steps are done first. Intervention needed authentication does not suit because re-authentication in the handoff needs intervention.

4.2 Kerberos

Kerberos is designed to provide authentication for client/server applications [1]. By using symmetric cryptography, Kerberos is a trusted third-party authentication protocol [16]. It benefits users by providing single sign on.

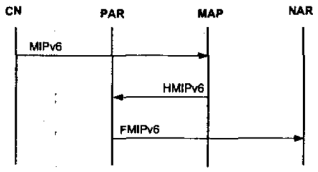

Figure 3: Signaling flow of the simple combination of HMIPv6 and FMIPv6 [12]

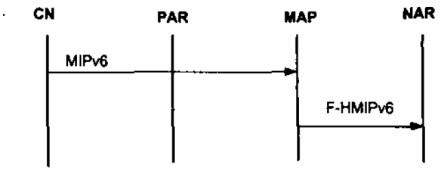

Figure 4: Effective signaling flow in F-HMIPv6 [12]

Kerberos divides AAA into two parts: Kerberos server and Ticket-Granting Server (TGS). First, the MN authenticates itself to Kerberos server and get a Ticket-Granting Ticket (TGT). Then, the MN sends a request with TGT to TGS when it wants to use certain services. The MN will receive a Service Ticket(ST) from TGS if the request is approved. Then the MN can use the service with the ST. On the other hand, the TGT data, which is created by Kerberos server when authentication, are also stored in TGS. In fact, the TGS is working as an access control center.

The delay of re-authentication in handoffs is reduced to zero because there is no re-authentication action. Either type of authentication suits for Kerberos also because of no re-authentication action. The MN gets trust just when they have correct TGT. Kerberos suits for small areas, where micro mobility protocols and nano mobility protocols are used, because the change of IP address is forbidden in Kerberos.

4.3 AP to AP credential

Another approach avoids to use AAA server or trusted third party in the re-authentication in order to avoid the time cost caused by communication with these servers [2]. The main idea of this approach is that the past honest behavior can assure the future behavior. Based on this belief, APs take the place of AAA server or trusted third party. When the MN authenticates to the first AP, the AP uses the common authentication process. When doing handoffs, the old AP sends the credential to the MN, the MN sends the credential to the new AP, and then the new AP checks the credential as some degree of authentication. The delay of handoffs only comes from two packets transmission between MN and the APs. Therefore, the performance of this approach is quite good.

In this approach, only the old AP, the new AP and the MN take part in the re-authentication. An essential requirement is that APs should trust each other. In order to trust the MN, the new AP only requires that the MN provides the credential from the old AP. If one MN abuses received credential, the whole network is suffered. On the other hand, the APs must have pre-shared secret or an agreed method to create new key to protect credential because the credential will be transferred by the MN. If using the trusted third party to protect the credential, the delay in the communication between the APs to trusted third party should make the whole approach meaningless.

In order to make APs trust each other, the above requirement requires that handoffs should happen in networks of the same organization. For wireless network, the scope of one organization

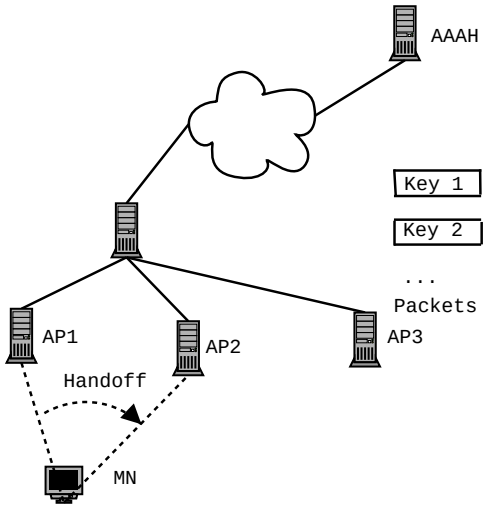

Figure 5: Key pre distribution

means micro mobility level or a limited macro mobility level. The optimization in this approach comes from reducing the delay of re-authentication. Either type of authentication suits for this approach since no real authentication in handoffs.

4.4 Localized authentications

In a localized network, we have three other choices because there is more trust in a localized network.

4.4.1 Key Pre-distribution to APs

One idea to get better performance in handoff processes is to reduce the delay of re-authentication by distributing the key material to the AP proactively. This idea is shown in Figure 5. When doing authentication, the AAA server creates different keys for different APs and saves these keys in packets. Every AP gets its own packet. When MN does handoff, the new AP just checks the content of the packet.

There are several approaches [19] [25] [14] which utilize the basic idea slightly differently. The performance improves evidently: for instance, Arunesh et al. at [19] say that the delay of re-authentication is reduced to 50 ms as the average while the delay of authentication is approx 800 ms.

The limitation is that APs must be trusted by the AAA server since they will receive the key beforehand. An approach which achieves the authentication in intra-network should be used. Another limitation is that every AP becomes the target of attack since they have the key to access the network.

Normally, these approaches use password based authentication while certificate based authentication is also able to be used here. Intervention needed authentication cannot be used here because the handoff needs re-authentication. Only micro mobility management and nano mobility management are suitable for these approaches since these approaches are based on the trust of localized network.

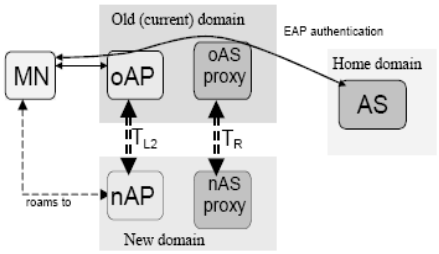

Figure 6: IAPP [4]

4.4.2 Predictive authentication

Compared to the solution in Section 4.3, predictive authentication scheme [20] chooses another way: to do authentications beforehand for a set of APs which are selected by An algorithm called Frequent Handoff Region (FHR) [20].

According to measurement results in [20], the average handoff latency is about 6 ms when using AAA local server and the latency is less than 20 ms when the AAA server is remote.

In this approach, to choose password based authentication or certificate based authentication makes no difference while intervention needed authentication cannot be used. But the design of FHR is very difficult and no good algorithm of FHR exists till now.

This approach is also only suitable for the micro mobility level and nano mobility level since FHR is designed based on localized network.

4.4.3 Authentication between APs

This type of approaches are very similar with the solution in Section 4.3. The participators are the same: the old AP, the new AP and MN. The main difference is that the credential is transferred between APs directly, but in AP to AP credential the credential for re-authentication is transferred by the path of "old AP - MN - new AP". These approaches benefit from doing re-authentication on above special way. Either type of authentication can be used. There are two existing approaches in this type of approaches.

- **Inter Access-Point Protocol**

  Compared to AP to AP credential in Section 4.3, in Inter Access-Point Protocol (IAPP) [15] APs must trust each other and this limits to a micro mobility or nano mobility area. The benefit is to avoid the cheat of MNs.

  Figure 6 shows the process of handoff in IAPP.

- **Context Transfer Protocol**

  Context Transfer Protocol (CXTP) [17] is an experimental protocol about handover. This approach has also three participators: MN, the new access router (nAR) and the previous access router(pAR). Each of them can start the process of handover. But the cryptographic information in handover process is only transferred between nAR and pAR. The performance can be increased much more by allowing MN attaching to nAR in advance.

5 Results

Table 1 shows how above approaches improve performance of the handoffs. Most approaches use various ways to reduce the delay of the re-authentication. However, HMIPv6 and F-HMIPv6 gain

	Method	Mobility Management	re-authentication	Latency
Mobile IP	FMIPv6	-	X	N/A
	HMIPv6	X	-	N/A
	F-HMIPv6	X	X	N/A
Kerberos		-	X	N/A
AP to AP credential		-	X	N/A
Localized Auth.	Pre-distribution	-	X	50 ms [19]
	Predictive authentication	-	X	<= 20 ms [20]
	Auth. between APs	-	X	N/A

Table 1: Sources of optimization in handoff processes and sample results from reference for various approaches (X = used; - = not used; N/A = not available)

benefit from amending the mobility management protocols.

Table 2 describes which types of authentication can be used for each handoff approach. The approaches, which try to reduce the delay of the re-authentication, can use both password based authentication and certificate based authentication. Intervention needed authentication only suits for those approaches which do not require a full authentication in the handoff process.

Table 3 concludes the difference between various approaches in scope. Localized authentication and kerberos are designed for micro mobility and nano mobility. This limitation gives more space for the design of these approaches and at the same time, the limitation comes with these approaches by nature. Mobile IP and AP to AP credential are suitable for the all mobility management levels. But not every approach in these categories can improve the performance of handoff process in all mobility management levels, e.g. HMIPv6 in macro mobility management.

6 Discussion

After analysis of above approaches, we can find that most current approaches are using password based authentication. To use password based authentication means the network should have AAA servers. The communication between APs and AAA servers should be protected by creating session keys. Password based authentication also requires different password for different systems or services. These properties make the collaboration between different operators difficult.

As aforementioned in Section 5, certificate based authentication can replace password based authentication in most of these approaches. PKI is one type of certificate based system. One big advantage is that PKI uses asymmetric cryptography and the public key is open to everyone. It brings a chance to do authentication between different operators easily. The other advantage is that PKI might become an important part in the future 3G network [13]. This means we can share PKI with other services to reduce the cost. One possibility of increasing performance is to build a local *Public Key Cache Server* (PKCS) to reduce the communication delay to the PKI. This PKCS is also able to be shared by many other services.

Certificate based authentication has one big limitation that the computation of asymmetric cryptography is much slower than symmetric cryptography. But this can be ignored when doing re-authentication by predictive authentication since the re-authentication happens before the real

	Method	Password based	Certificate based	Intervention needed
Mobile IP	FMIPv6	X	X	-
	HMIPv6	X	-	-
	F-HMIPv6	X	X	-
Kerberos		X	X	X
AP to AP credential		X	X	X
Localized Auth.	Pre-distribution	X	X	-
	Predictive authentication	X	X	-
	Auth. between APs	X	X	X

Table 2: Various types of authentication in handoff processes for different approaches (X = can be used; - = cannot be used)

	Method	Macro Mobility	Micro Mobility and Nano Mobility
Mobile IP	FMIPv6	X	X
	HMIPv6	*	XX
	F-HMIPv6	X	XX
Kerberos		-	XX
AP to AP credential		X	XX
Localized Auth.	Pre-distribution	-	XX
	Predictive authentication	-	XX
	Auth. between APs	-	XX

Table 3: Results of comparing various approaches by mobility management level (X = to increase performance; XX = to increase handoff performance notably; * = can work, but no performance increase; - = can not work)

handoff and its time cost will not be calculated into the delay of handoffs, or by authentication between APs since no real authentication process during this process.

We suggest one solution based on the above issues.

1. Asymmetric cryptography is used in authentication. PKI provides the public key.
2. A PKCS, which stores the public key locally, is created in order to reduce delay of communication between the public key holder and APs.
3. Various methods are supported to gain optimization in handoff.
   (a) APs, selected by using a Frequent Handoff Region (FHR) like predictive authentication in Section 4.4.2, could get the public key of MN beforehand.
   (b) Authentication could be done before layer 2 handoff.

4. Other benefits by using PKI.

   (a) APs could also authenticate to MN .

   (b) Intra operator trust could be built on the hypothesis: each AP has its own certificate.

   (c) External operator communication could use asymmetric cryptography to protect data between different operators.

The above approach lies on the establishment of the PKI. If PKI is established all over the world, the cost will be very small since other services can also uses this infrastructure.

However, this idea has some problem open. For example, key revocation may happen to public keys stored in PKCS. We have to create a way to let PKCS notice key revocation. We leave these questions to future work.

7 Conclusions

In this paper, we analyze various fast solutions of handoff between APs. Scope and the type of authentication are considered. We pay attention to the sources of optimization on different solutions. Finally, we suggest a solution based on our analysis result.

Acknowledgement

We would like to thank Janne Lindqvist, Ursula Holmström, and three anonymous reviewers for their constructive comments. We also thank Antti Ylä-Jääski for his selfless support during the whole process.

References

[1] ANON. Kerberos: The network authentication protocol, 2005.

[2] T. Aura and M. Roe. Reducing reauthentication delay in wireless networks. In *Proceedings of IEEE SecureComm 2005*, Athens, Greece, 2005.

[3] S. Auvray. Fast Handovers for Mobile IPv6. EURESCOM Participants in Project P1113, 2002.

[4] M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang, and P. Schoo. Fast authentication methods for handovers between IEEE 802.11 wireless lans. In *WMASH 04*, Philadelphia, Pennsylvania, USA, 2004.

[5] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko. Diameter Base Protocol, September 2003. RFC 3588.

[6] J. Edney and W. A. Arbaugh. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Addison-Wesley, 2003.

[7] S. Glass, T. Hiller, S. Jacobs, and C. Perkins. Mobile IP authentication, authorization, and accounting requirements, October 2000. RFC 2977.

[8] R. Housley and B. Aboba. AAA Key Management. draft-housley-aaa-key-mgmt-01.txt (work in progress), June 2005.

[9] A. K. Jain, , A. Ross, and S. Prabhakar. An Introduction to Biometric Recognition. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 14(1), January 2004.

[10] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom. Picture Password: A Visual Login Technique for Mobile Devices. National Institute of Standards and Technology Interagency Report (NISTIR) 7030, July 2003.

[11] D. Johnson, C. Perkins, and J. Arkko. RFC3775: Mobility Support in IPv6, June 2004. Status: STANDARD.

[12] H. Jung and S. Koh. Fast handover support in hierarchical mobile ipv6. In *Advanced Communication Technology, 2004. The 6th International Conference on Volume 2*, pages 551 – 554, 2004.

[13] G. Kambourakis, A. Rouskas, and S. Gritzalis. Inter/Intra Core Network Security with PKI for 3G-and-Beyond Systems. In *NETWORKING 2004*, pages 13–24, Athens, Greece, May 2004.

[14] M. Kassab, A. Belghith, J.-M. Bonnin, and S. Sassi. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. In *WMuNeP '05: Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling*, pages 46–53, New York, NY, USA, 2005. ACM Press.

[15] S. Kerry, D. Bagby, and B. O'Hara. Recommended practice for multi-vendor of access point interoperability via an inter-access point protocol across distribution systems supporting ieee 802.11 operation. IEEE 802.11f/D5, 2003. Draft.

[16] J. Kohl and C. Neuman. The kerberos network authentication service (v5), September 1993. RFC 1510.

[17] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli. Context transfer protocol (cxtp), July 2005. RFC 4067.

[18] J. Manner and M. Kojo. Mobility related terminology, 2004. RFC 3753.

[19] A. Mishra, M. H. Shin, N. L. Petroni, Jr., T. C. Clancy, and W. A. Arbaugh. Proactive key distribution using neighbor graphs. *IEEE Wireless Communications Magazine*, February 2004.

[20] S. Pack and Y. Choi. Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN. Atlanta, USA, 2002. Springer Verlag.

[21] C. Perkins. IP mobility support for ipv4, August 2002. RFC 3344.

[22] C. Perkins and P. Calhoun. Authentication, authorization, and accounting (AAA) registration keys for mobile ipv4, 2005. RFC 3957.

[23] C. E. Perkins. *MOBILE IP - Design Principles and Practices*. Prentice Hall PTR, Jan 1998.

[24] E. R. Koodli. Fast handovers for mobile ipv6, July 2005. RFC 4068.

[25] M. Ramkumar. Broadcast Encryption with Random Key Pre-distribution Schemes. Cryptology ePrint Archive, May 2005.

[26] R. J. B. Reynolds and A. W. Rix. Quality VoIP - An Engineering Challenge. *BT Technology Journal*, 19:23–32, 2001.

[27] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote authentication dial in user service (radius), June 2000. RFC 2138.

[28] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier. Hierarchical mobile ipv6 mobility management (hmipv6), August 2005. RFC 4140.

[29] K. Sötti and P. Kyheränen. A Hierarchical Mobile IPv6. EURESCOM Participants in Project P1113, 2002.

[30] M. Stemm. Vertical handoffs in wireless overlay networks. Technical Report UCB/CSD-96-903, EECS Department, University of California, Berkeley, 1996.