EAP-Kerberos: Leveraging the Kerberos Credential Caching Mechanism for Faster Re-authentications in Wireless Access Networks

Saber Zrelli
Nobuo Okabe
Corporate R&D Headquarters
Yokogawa Electric Corporation
Tokyo, Japan
saber.zrelli,nobuo.okabe@jp.yokogawa.com

Yoichi Shinoda
Center for Information Science
Japan Advanced Institute of Science and Technology
Ishikawa, Japan
shinoda@jaist.ac.jp

***Abstract*—Although the wireless technology nowadays provides satisfying bandwidth and higher speeds, it still lacks improvements with regard to handoff performance. Existing solutions for reducing handoff delays are specific to a particular network technology or require expensive upgrades of the whole infrastructure. In this paper, we investigate performance benefits of leveraging the Kerberos ticket cashing mechanism for achieving faster re-authentications in IEEE 802.11 wireless access networks. For this purpose, we designed a new EAP authentication method, EAP-Kerberos, and evaluated re-authentication performance in different scenarios.**

***Keywords*-Wireless; Authentication; Handoff; Performance**

I. INTRODUCTION

Mobile wireless stations perform handoffs in order to change their point of attachment to the network. A handoff from an old access point to a new access point involves several steps that each may introduce delays.

A. What causes handoff delays

Handoff latency has long been an acknowledged issue in wireless networks. Some of the experimental studies [1] [2] have attributed the handoff delay in wireless local area networks (IEEE 802.11) to the scanning phase during which a wireless station discovers neighboring access points. These studies however, did not take authentication delays into consideration. In a previous work [3], we have shown that authentication using the Extensible Authentication Protocol [4] can take substantial delays especially when authentication servers are located in remote locations far from the access point.

B. How security impacts handoff delays

The Extensible Authentication protocol (EAP), is a core component in standard AAA (Authentication Authorization and Accounting) frameworks for access control in various network technologies such as 802.3, 802.11 and 802.16. In these frameworks, EAP authentication delays may become an issue especially in roaming situations; AAA frameworks support cross-domain authentication that enables an access network to authenticate a roaming client that belongs to a remote domain. The cross-domain authentication requires message exchange between the AAA server of the visited network and the AAA server of the roaming station's home network. Because these inter-domain exchanges occur over the Internet, they are subject to degradations such as packet loss and network delays which increases the overall authentication time. When a roaming station changes of access point, the same authentication procedure takes place again, disrupting the user traffic at each handoff.

C. Contributions

In this paper, we investigate performance benefits from using the Kerberos authentication protocol within wireless authentication frameworks that rely on the Extensible Authentication Protocol (EAP).

By relying on the legacy Kerberos authentication protocol as defined in [5], our scheme provides the same security properties as Kerberos and inherits its highly prized performance and simplicity. There are several aspects in the design of the Kerberos protocol that makes it suitable for use as the underlying authentication mechanism in wireless networks where handoff performance is a desired property. First, the Kerberos protocol uses symmetric key cryptography which consumes much less computing resources and hence introduces less delays compared to common methods based on public key cryptography. Second, the use of *Tickets* in Kerberos allows the client to perform fast re-authentication through a two round-trips exchange with the local authentication server, without the need for contacting any remote entity even if the client is in a roaming situation (i.e. The client belongs to a domain different from the domain that owns the local access network).

II. IEEE 802.1X EAP AUTHENTICATION

In order to gain access to the infrastructure, a wireless station (STA) needs to authenticate and share a key with the

 ISBN: 978-1-61208-100-7

Access Point (AP) using the *Extensible Authentication Protocol (EAP)* [6] and IEEE 802.1X. During EAP authentication, the AP acts as a pass-through between the STA and a back-end authentication server. As shown in Figure 1, EAP packets are transported over IEEE 802.1X between the AP and the STA in the front-end side, and using a AAA (Authentication Authorization and Accounting) protocol such as RADIUS [7] [8] or Diameter [9] [10] between the AP and the authentication server in the back-end side. After a successful authentication, the STA and the authentication server derive a shared key called *Master Session Key (MSK)*. Finally, the the back-end authentication server sends the MSK to the AP along with a notification of successful authentication.

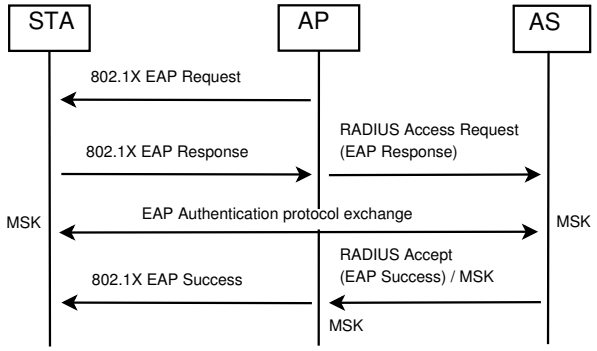


Fig. 1: IEEE 802.1X/ EAP authentication

III. The Kerberos Authentication Protocol

Kerberos [5] is a widely deployed authentication system. The authentication process in Kerberos involves *principals* and a *Key Distribution Center (KDC)*. Principals represent users and services registered in the Kerberos domain or realm. The KDC maintains a database of principals and shares a secret key with each one of them. In order to access an actual service, the client must submit valid Kerberos credentials to the service.

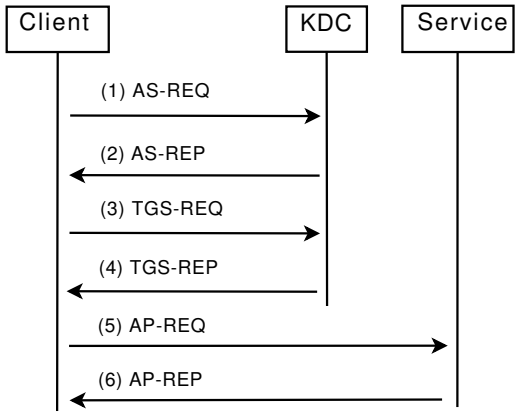


Fig. 2: The Kerberos authentication exchange

The Kerberos protocol specifies three exchanges, the *Authentication Server (AS) exchange*, the *Ticket Granting Service (TGS) exchange* and the *Client Server (AP) exchange*. The three exchanges are depicted in Figure 2. The AS exchange allows the client to obtain credentials that it can use to prove its identity to the KDC. These credentials consist of a Ticket referred to as *Ticket Granting Ticket (TGT)*, and a session key referred to as *TGS session key*. A Ticket is a message created by the Kerberos key distribution center and encrypted using the secret key of the target service.

The TGS exchange, on the other hand, allows the client to authenticate to the KDC using the TGT and to obtain a Ticket for a certain service. After validating the client request (TGS-REQ), the KDC issues a Ticket for the client and sends it along with the associated session key in a TGS Reply message (TGS-REP).

The AP exchange is performed between the client and the service to authenticate the client before granting it access to the resources. The client initiates the authentication by issuing an AP Request message (AP-REQ) that contains a Ticket for the service. After validating client's credentials the service authorizes the client and optionally sends an AP Reply message (AP-REP) to achieve mutual authentication.

IV. The EAP Kerberos Authentication Method

The EAP-Kerberos authentication method allows network clients to use Kerberos credentials to achieve mutual authentication with back-end authentication servers in wireless access networks.

The EAP-Kerberos method requires that each network access providers deploys a Kerberos realm with one or more Key distribution centers and that network clients are registered in the Kerberos principals database. In order to gain network access, a wireless station must possess a Kerberos login and password pair that can be used to authenticate the station to the network access provider's Kerberos KDC.

In the following sections, we present the design and operations of the EAP-Kerberos authentication method.

A. Overview

Our approach for using Kerberos in network access control is based on the notion of *Network Access Zones* that we define as a collection of lightweight access points managed by a single back-end authentication server. A set of network access zones that belong to the same provider constitutes an Access Network. Although an average sized access network may consist of a single network access zone, the partitioning of the access network into different zones is important for larger access networks such as those of wireless Internet providers. Generally, the use of multiple zones in large access networks makes management easier and ensures a scalable infrastructure.

To each network access zone corresponds a Kerberos service registered in a Kerberos key distribution center managed by an access network provider. Furthermore, the authentication server managing a certain zone has the secret Kerberos key of the corresponding zone. This secret key shared with the KDC

 ISBN: 978-1-61208-100-7

allows the authentication server to validate Kerberos AP-REQ messages it receives over EAP from wireless clients that are requesting access in the zone.

In order to gain network access within a zone, a wireless station must obtain a service Ticket for the local network access zone and present the Ticket to the zone's authentication server. The EAP-Kerberos method described hereafter specifies how the station obtains Kerberos credentials and how it uses them to authenticate and gain network access.

B. Station behavior

The STA and the authentication server negotiate the use of the EAP-Kerberos method as they would do for legacy EAP methods [6]. After a station have initiated the EAP-Kerberos method, the first message issued by the authentication server includes the Kerberos realm name as well as information identifying the local network access zone (see Section IV-A for the definition of network access zones). This information represented by REALM and ZONE in Figure 3 constitutes the local zone's Kerberos principal name that uniquely identifies it within the global Kerberos name space.

Upon reception of this first message, the STA checks its Kerberos credential cache for service Tickets and Kerberos Ticket Granting Tickets. Depending on what credentials are available, the station's behavior varies as follows.

1) Service Ticket for the local zone available: If the station has a Kerberos service Ticket for the local zone in its credential cache, then the STA initiates a Kerberos AP exchange over EAP with the authentication server managing the local zone.

2) Ticket Granting Ticket for local realm available: If the STA does not have a Ticket for the zone, but has a Ticket Granting Ticket for the local zone's Kerberos realm, then the STA must acquire a Ticket by performing a Kerberos TGS exchange with the Key Distribution Center where the zone is registered. The TGS exchange is tunneled in EAP between the STA and the local zone's authentication server. From there, the local zone's authentication server proxies the TGS exchange between the STA and the Kerberos KDC. For this purpose, the authentication server extracts the TGS-REQ message from the EAP-Kerberos message issued by the STA and sends it to the Kerberos KDC. The reply message from the KDC is sent back to the STA in an EAP-Kerberos message. After obtaining the service Ticket, the STA can perform an AP exchange with the authentication server.

3) No tickets available: If the STA does not have a service Ticket for the zone nor a TGT for the local realm, then it first needs to obtain a TGT for the local realm. The process of obtaining a TGT for the local realm depends on whether the Kerberos realm where the zone is registered is the same as the STA's home Kerberos realm or not. In the former case, the STA uses an AS exchange with the Kerberos KDC of the local realm. In the latter case, the STA first gets a TGT for its

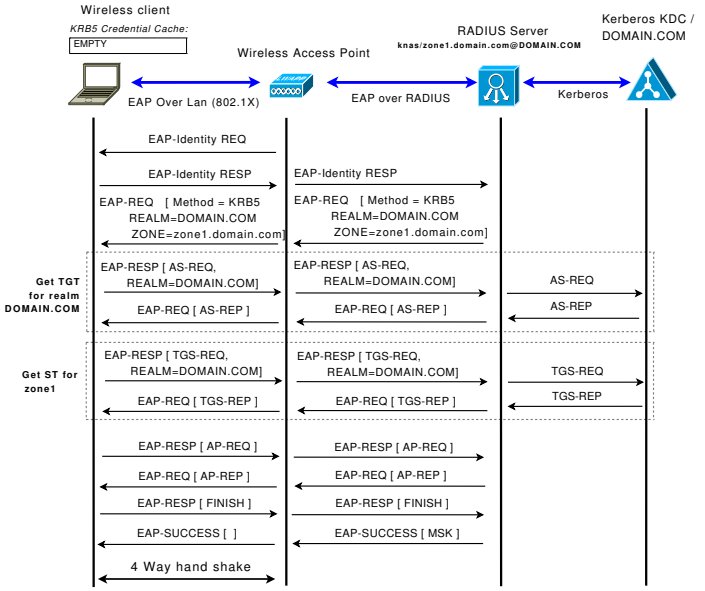


Fig. 3: Initial EAP-Kerberos authentication in the home access network

home Kerberos realm using an AS exchange with its home KDC, then, the STA performs Kerberos cross-realm TGS exchanges as specified in [5]. After the STA has obtained a TGT for the local realm, it performs a TGS exchange with the local realm's KDC to obtain a service Ticket for the local zone, then, it initiates an AP exchange with the local zone's authentication server to achieve mutual authentication and gain network access.

C. Use cases

When a STA is booted or is performing a handoff from an access point to another, it follows the same behavior described in Section IV-B. In the following, we provide more details and illustrate how the EAP-Kerberos method works in different use cases.

1) Initial authentication in the home network: The first use case we consider is the case where the STA needs to gain network connectivity through a network access zone that belongs to the station's home domain (e.g, when a subscriber is using her ISP's infrastructure). If the STA does not possess any cached Kerberos credentials for network access, then it needs to carry out three Kerberos exchanges; AS and TGS exchanges with the Kerberos KDC and an AP exchange with the authentication server managing the local network access zone.

As shown in Figure 3, the STA receives the Kerberos realm name (REALM) as well as the current zone's principal name (ZONE) in the initial EAP-Kerberos message issued by the zone's RADIUS authentication server. Since the STA does not possess any credentials yet, it first obtains a TGT using an AS exchange relayed by the access network infrastructure to

 ISBN: 978-1-61208-100-7

the STA's home Kerberos KDC. The EAP-Kerberos message carrying the AS-REQ message also contains the Kerberos realm name of the STA's home KDC. This information, will be used by the RADIUS server to locate the IP address of the Kerberos KDC to which the Kerberos message must be forwarded. In practice, IP addresses of Kerberos KDCs are resolved from Kerberos realm names using DNS SRV records[11] or mappings using static configuration files.

After obtaining the TGT, the STA requests a service ticket for the service "knas/zone1.domain.com@DOMAIN.COM". For this, the STA performs a TGS exchange with the Kerberos KDC of the current zone. As with the AS exchange, the TGS exchange is relayed by the RADIUS authentication server. The STA then initiates an AP exchange to authenticate with the RADIUS server managing the network access zone. After the AP exchange is completed, the STA issues a FINISH message to indicate to the RADIUS server that mutual authentication has been established. The authentication server then sends the EAP Master Session Key (MSK) to the AP. Finally, the STA and the AP use the shared MSK to establish a security association. In the case of IEEE 802.11, they perform the four-way handshake to derive Transient Session Keys from the MSK.

2) Intra-zone Handoff: The first handoff scenario we consider consists of the mobile STA's handoff within the same network access zone. In this case, the STA does not need to acquire new credentials since it already has a Ticket for the local zone (unless when the Ticket has expired). The authentication with the access network only requires an AP exchange with the local authentication server.

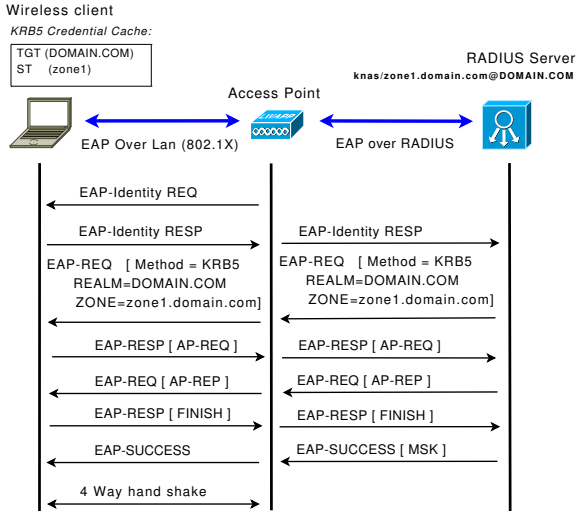


Fig. 4: EAP-Kerberos re-authentication in an Intra-zone handoff: The STA re-uses the Kerberos ticket for the current access network zone to re-authenticate with the RADIUS server.

As shown in Figure 4, the authentication, including all EAP messages, uses 3.5 round trips. All messages are exchanged within the zone and no entities in remote locations are involved in the intra-zone handoff process.

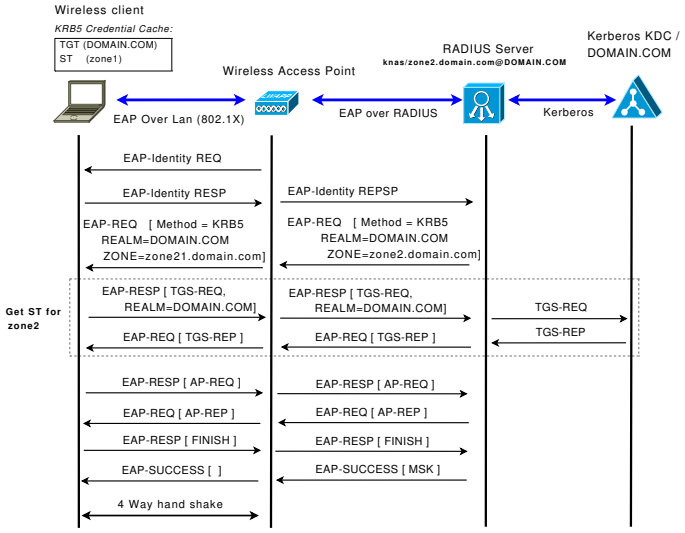


Fig. 5: EAP-Kerberos authentication in an Inter-zone handoff: The STA re-uses the TGT for the local realm to obtain a ticket for the new zone and authenticate with the RADIUS server.

3) Inter-zone Handoff: When the STA moves to a new access network zone, it may need to acquire a new Ticket for the new zone. If the new zone belongs to the same access network as the previous zone, the STA can re-use the TGT for the local realm to obtain a service Ticket for the new zone then authenticate with the new zone's authentication server. The inter-zone handoff scenario, as shown in Figure 5, requires an additional round-trip (for a total of 4.5) in comparison to the intra-zone handoff scenario.

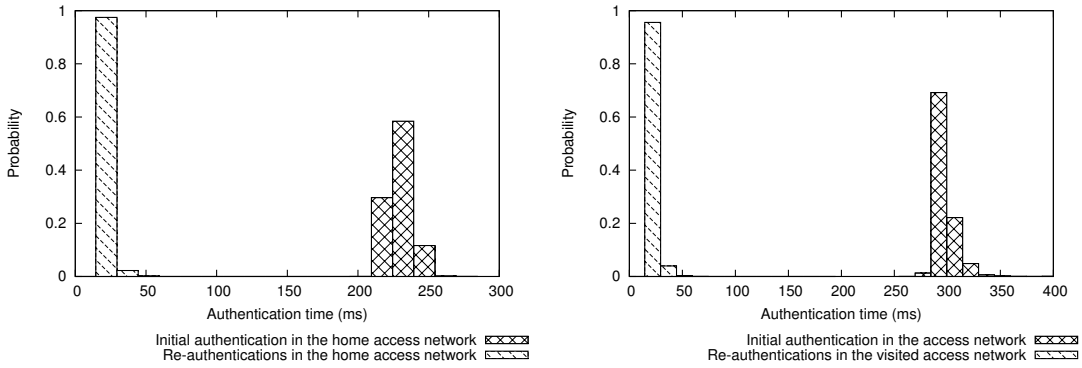
V. Performance Evaluation

We implemented the EAP-Kerberos method by extending the open-source *hostapd* [12] RADIUS server and the *wpa_supplicant* [13] EAP supplicant. For comparison, we performed performance evaluation of the EAP-PEAPv0 authentication method using Microsoft Windows 2003 server's Internet Authentication Server (IAS) on the same test-bed.

The test-bed consisted of two access networks, each composed of one network access zone. The two network access zones belong to different Kerberos realms and each has its own RADIUS authentication server and Kerberos Key Distribution Center. In order to emulate network delays, we used the Linux *netem* [14] utility. The resulting test-bed was equivalent to the reference architecture depicted in Figure 6.

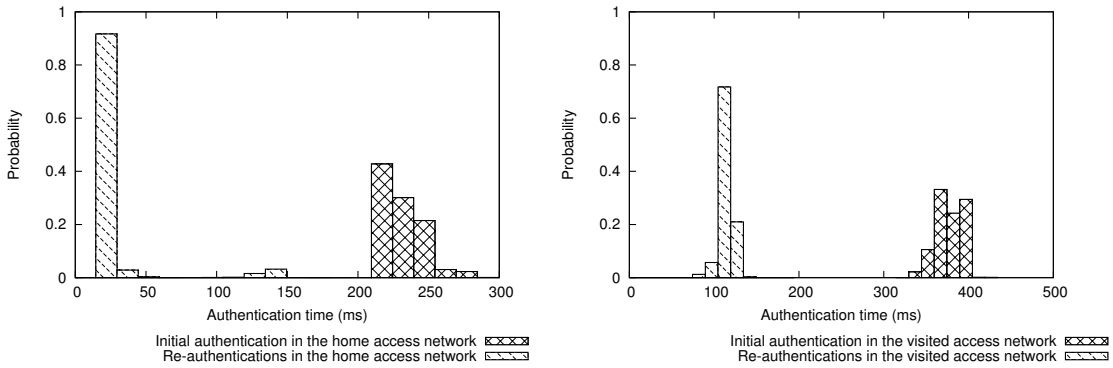
Figure 7 shows authentication delays using the EAP-Kerberos method in different scenarios. The re-authentication delay with EAP-Kerberos (30ms) is the same whether the wireless station is in its home network or in a visited network. When comparing intra-zone re-authentication delays in the home access network for the EAP-PEAPv0 method (Figure 8a)

 ISBN: 978-1-61208-100-7



(a) EAP-Kerberos performance in the home access network (b) EAP-Kerberos performance in the visited access network

Fig. 7: Probability Density Functions of re-authentication delays for the EAP-Kerberos authentication method



(a) EAP-PEAPv0 performance in the home access network (b) EAP-PEAPv0 performance in the visited access network

Fig. 8: Probability Density Functions of re-authentication delays for the EAP-PEAPv0 authentication method

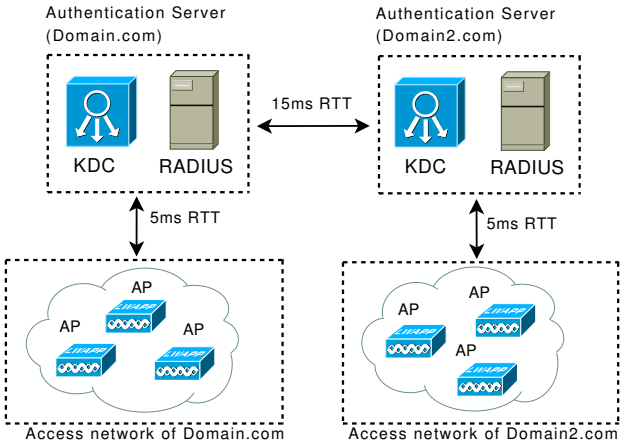


Fig. 6: Reference architecture

and the EAP-Kerberos method (Figure 7a), we can notice that both methods offer similar performance. However, in roaming scenarios when the station is performing handoffs in a visited access network, the EAP-Kerberos method shows superior performance.

As shown in Figure 7b, intra-zone re-authentication delays remained acceptable in the roaming case for EAP-Kerberos (30ms) while re-authentication latency increased about four folds from 30ms to around 120ms for EAP-PEAPv0 (Figure 8b). This is due to the fact that EAP-PEAPv0 (as it is the case for all legacy EAP authentication methods) require message exchange with the roaming station's home RADIUS server for performing re-authentications in foreign access networks while the EAP-Kerberos method involves only entities in the the visited access network.

VI. Conclusion

In order to achieve true ubiquitous applications, the handoff delays in wireless networks must be kept to the minimum. Several steps in the handoff process may be subject to enhancements. In this paper, we consider authentication delays during handoffs. The problem with handoff latency arises when a roaming wireless station performs handoffs in a foreign access network. The inter-domain exchanges necessary for

 ISBN: 978-1-61208-100-7

authenticating the roaming station may introduce large delays that would affect quality of service in real-time applications.

We have designed, implemented and evaluated a Kerberos-based EAP authentication method that achieves strong authentication with reduced latency during handoffs. Experimental results from our test-bed show that EAP-Kerberos re-authentications in roaming scenarios took around 30 milliseconds, more than 3 times faster than EAP-PEAPv0 that took around 120 milliseconds.

When compared to existing solutions for reducing EAP re-authentication delays such as IEEE 802.11r [15] and ERP [16], the approach presented in this paper has three main advantages; (1) The proposed method extends the EAP layer by specifying a new EAP method which ensures that the proposed approach is link layer independent. (2) The proposed approach does not require changes in the access point, and therefore it has an advantage from deployment cost point of view, and (3) The EAP method proposed in this paper supports fast inter access point and inter access network handoffs by relying on Kerberos cross-realm authentication capabilities. Other existing approaches enable fast re-authentication only within the same access network.

REFERENCES

[1] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 mac layer handoff process," SIGCOMM Comput. Commun. Rev., vol. 33, no. 2, pp. 93–102, 2003.

[2] H. Velayos and G. Karlsson, "Techniques to reduce the IEEE 802.11b handoff time," Tech. Rep., 20-24 June 2004.

[3] S. Zrelli and Y. Shinoda, "Experimental evaluation of EAP performance in roaming scenarios," in Sustainable Internet, Third Asian Internet Engineering Conference, ser. Lecture Notes in Computer Science, S. Fdida and K. Sugiura, Eds., vol. 4866. Springer, 2007, pp. 86–98. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-76809-8_8

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748 (Proposed Standard), Jun. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3748.txt

[5] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," RFC 4120 (Proposed Standard), Internet Engineering Task Force, Jul. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4119.txt

[6] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748 (Proposed Standard), Jun. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3748.txt

[7] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865 (Draft Standard), Internet Engineering Task Force, Jun. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2865.txt

[8] B. Aboba and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)," RFC 3579 (Informational), Sep. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3579.txt

[9] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," RFC 3588 (Proposed Standard), Internet Engineering Task Force, Sep. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3588.txt

[10] P. Eronen, T. Hiller, and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," RFC 4072 (Proposed Standard), Internet Engineering Task Force, Aug. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4072.txt

[11] A. Gulbrandsen, P. Vixie, and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)," RFC 2782 (Proposed Standard), Feb. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2782.txt

[12] "hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator," Web page, As of July 2010. [Online]. Available: http://hostap.epitest.fi/hostapd/

[13] "Linux WPA/WPA2/IEEE 802.1X Supplicant," Web page, As of July 2010. [Online]. Available: http://hostap.epitest.fi/wpa_supplicant/

[14] "Netem: The Linux Network Emulator," Web page, As of July 2010. [Online]. Available: http://www.linuxfoundation.org/collaborate/workgroups/networking/netem

[15] 802.11r, "IEEE Standard for Information technology, Telecommunications and information exchange between systems, Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition," IEEE Standards, 2008. [Online]. Available: http://dx.doi.org/10.1109%2FIEEESTD.2008.4573292

[16] V. Narayanan and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," RFC 5296 (Proposed Standard), Aug. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5296.txt

 ISBN: 978-1-61208-100-7