Proactive Key Delivery for Fast Authentication in WLAN-based Access Networks

Ha Hoang Duong, Arek Dadej and Steven Gordon
Institute for Telecommunications Research, University of South Australia
Email: Ha.Duong@postgrads.unisa.edu.au, {Arek.Dadej, Steven.Gordon}@unisa.edu.au

Abstract – In this paper, we propose a method for proactive key delivery to enable fast authentication as wireless LAN nodes move between Access Points within an administrative domain. The method optimises the EAP-TLS phase of the IEEE 802.11i authentication process by creating list of keys at the first authentication with the administrative domain, and proactively delivering those keys to candidate Access Points. This takes advantage of Proactive Context Transfer and Forced Handover. The performance analysis shows that the proposal can reduce significantly authentication delay and bandwidth consumption; hence improve overall handover performance.

I. Introduction

The common availability of third generation mobile networks and, particularly Wireless LANs (WLAN) have made wireless networking an increasingly important and popular way of providing Internet access to users on the move. However, the mobility of wireless users has also created a number of technological challenges, especially when a Mobile Node (MN) changes the point of network access (i.e. performs handover to a new access network). As a consequence of the handover, the MN must re-establish services associated with the access network to enable truly seamless handovers.

An important service deployed in any network is authentication. The heart of the authentication process is a shared secret between the user and an authentication server (AS), used to verify the user's identity and to determine the user's right to access resources and services. Typically, the shared secret is used by different authentication protocols to generate keys for various purposes such as mutual authentication, message protection, and secure transmission.

Authentication can be a time and bandwidth consuming process. Therefore it is undesirable to continually have to re-authenticate as a mobile node changes points of access (e.g. handover). An approach of fast proactive authentication, where necessary authentication information is transferred between access points before the handover, has been the topic of interest by many researchers (see [16] for a summary). Our proposal is within this topic.- here we want to mention two methods close to our proposal, namely Frequent Handover Region (FHR) in [17] and Neighbour Graph (NG) in [1]. The idea of FHR method is to build FHR for every Access Point (AP) based on the record of previous handovers with a weighted matrix and to distribute keys to all APs of FHR in advance. An issue with the scheme is the size of FHR. The probability of MN performing handover with one of the APs from a FHR depends on the size of the FHR, i.e. larger size can give higher probability. Consequently, the FHR covers more APs for proactive key distributions, and such a flood of key distribution may overwhelm the AS. The construction of a weighted matrix requires $O(m^2)$ computation and space, where m is the number of APs in the network; hence can also pressure the AS. Mishra [1] suggested an improvement by using NG to distribute keys one hop in advance. However, as the distributed keys are derived from the key with the current AP, the NG method requires a trust relationship between APs, which is an undesirable security assumption in many environments..

Our proposal has a similar approach to FHR and NG of proactive key delivery, but is different in the way of selecting APs for key distribution. The proposal is an application of our previous work, the proactive scheme of Context Transfer and Forced Handover in [7] [8], into the authentication service.

The rest of the paper is structured as follows. In the next section, we provide background information in IEEE 802.11 WLANs. Then, we present the proposal of proactive key delivery, and analyse its performance in sections III and IV. Finally, we make concluding remarks and comment on questions for near future investigation in the last section.

II. Background in IEEE 802.11 WLAN

In this section, we give an overview of signal strength based handover algorithm, the IEEE 802.11i authentication service, and the scheme of proactive Context Transfer and Forced Handover in 802.11 WLAN.

A. Signal Strength-Based Handover

In an 802.11 WLAN, a MN leaving an AP is required to find the next AP and re-associate (i.e. perform handover to this AP). A fundamental question is: when does the MN need to switch from one AP to another? In most implementations, for example in [14], quality of the communication link is used to make the handover decision, however more advanced decisions can be made by also taking into account the AP load, e.g. as in [6]. Figure 1 shows how the typical parameter of communication quality, signal-to-noise ratio (SNR), changes as a MN moves from AP1 to the adjacent AP2. As soon as *SNR* from AP, SNR_1, drops below the so-called Cell Search Threshold SNR_{CST} (point 1 in Figure 1), the MN enters the "cell-search" state where it scans to find the better APs. In the scanning process, for every channel, the MN broadcasts Probe Request and waits for Probe Response from

AP. The scanning process is repeated every Scanning Interval (T_{SI}) until one of scanned APs provide *SNR* at least Δ greater than the current *SNR* (point 4 in Figure 1). Now, the MN can switch to the channel used by the selected AP, and start the reassociation process. In summary, the condition for the inter-AP handover is as follows

$$\begin{cases} SNR_1 < SNR_{CRT} \\ SNR_2 > SNR_1 + \Delta \end{cases} \quad (1)$$

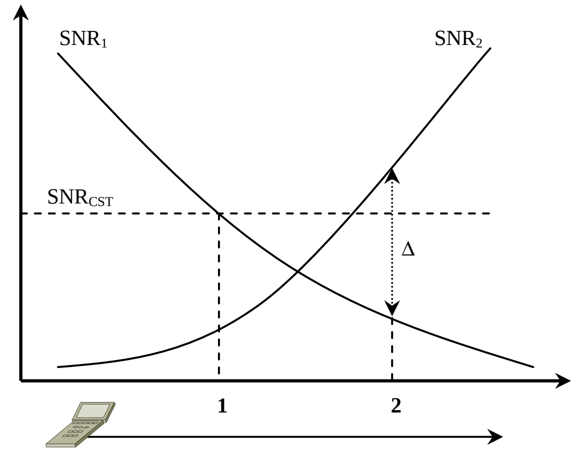

Figure 1 SNR change between AP1 and AP2

B. IEEE 802.11i Authentication

Initially, the IEEE 802.11 standard [10] specified two authentication methods, open system authenticating allowing any user to access the network, and shared key, e.g. WEP. Limitations of WEP [19] have led to the IEEE 802.11i security framework [9], which replaces the authentication using 802.11 frames with higher layer authentication protocols. Messages of the 802.11i framework are exchanged immediately after re-association, but to maintain backward compatibility, open system authentication still takes place before re-association.

The 802.11i framework is a complex combination of several different protocols. In 802.11i three entities participate in the authentication process, the supplicant (i.e. a MN that requests access), the authenticator (i.e. an entity that is typically located in AP and controls access gate), and the authoriser (i.e. AS that decides whether the supplicant is to be accepted). Figure 2 shows the 802.11i framework that includes three layers, MAC layer, access control layer and authentication layer.

- The MAC layer (e.g. 802.11) is to deal with raw communication, and advertising capabilities.
- The access control layer (i.e. 802.1X Port Access Control [11], Extensible Authentication Protocol (EAP) [13], Remote Authentication Dial-In User Service (RADIUS) [4] and their extensions, EAP over LAN (EAPOL) [11], EAP over RADIUS [5]) is to make sure that only authorized MNs can communicate with the network.
- The authentication layer (i.e. Transport Layer Security (TLS) [18] and its extension, EAP-TLS [2]), is responsible for making policy decision, and accepting (or rejecting) request of a MN to join to the network.

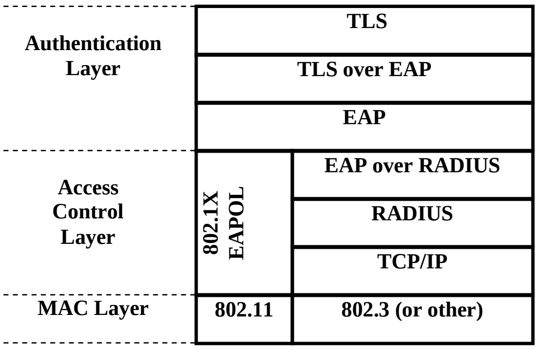

Figure 2 Protocol Stack of IEEE 802.11i framework

The basic process of 802.11i authentication is as follows (see Figure 3):

- Assuming both MN and AS hold the same shared key, an initial mutual authentication between the two entities is performed (steps 1 to 8).
- Using the secret key and a preknown function, the MN and AS generate a Master Key (MK) that will be used for future exchanges (so that the secret key is no longer in use).
- From the MK, a Pairwise Master Key (PMK) is then generated and sent from AS to the AP (step 11) so it can also participate in the communications. The MN, AP and AS all have the PMK for this session.
- The MN then authenticates with the AP in a four way handshake, which includes derivation of a Pairwise Transient Key (PTK) which can be used in subsequent communications between MN and AP.

As can be seen in Figure 3, the protocols used necessitate various message exchanges to implement the above authentication steps. Normally these steps must be undertaken whenever a MN hands over between APs. As we will show shortly, some of these steps can be reduced by proactively transferring PMK’s to potential APs before a handover.

C. Proactive Context Transfer and Forced Handover

In [7] and [8], we proposed a scheme of proactive Context Transfer and Forced Handover for WLAN-based access networks. The key point of this scheme is to identify the best moment for Context Transfer, and to force handover at a planned time as follows.

Entering scanning cycles, the MN estimates time until handover T_{UH}

$$T_{UH} = \frac{\Delta - (SNR_2 - SNR_1)}{R_{SNR2} - R_{SNR1}} \qquad (2)$$

where R_{SNR1} and R_{SNR2} are rates of SNR change for signals from the current AP and the scanned AP respectively. These rate values are obtained and updated on the basis of SNR measurements performed as part of the current and previous scanning cycles.

The estimations are carried out at every scanning cycle until $T_{UH} < T_{SI}$ is eventually achieved at a scanning cycle (called scanning-to-Context Transfer). Immediately after this cycle, the MN collects MAC addresses of APs satisfying ($T_{UH} < T_{SI}$)

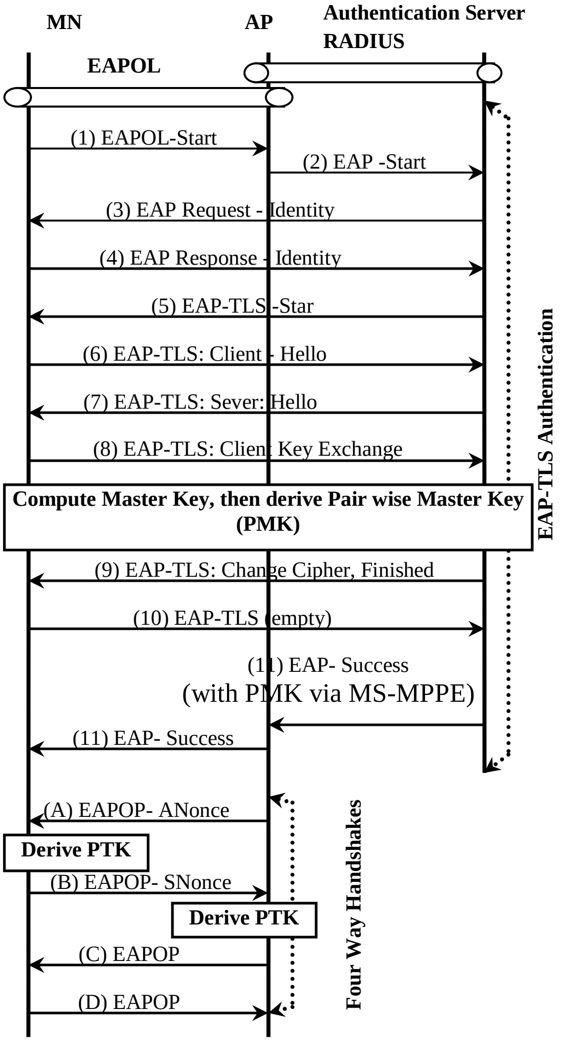

Figure 3 The complete set of messages in EAP-TLS and four-way handshake processes.

(i.e. candidate APs) and uses Candidate Access Router Discovery (CARD) protocol [15] and Context Transfer Protocol (CTP) [12] to re-establish services at new access network including candidate APs, and possibly candidate ARs. For details of those operations, readers are referred to [7] and [8]. It is also emphasised that Context Transfer is a quick alternative to re-establish services associated between MN and access network.

III. Proposal of proactive key delivery

In this section, we present the basic idea of optimisation of the EAP-TLS, and then describe the process of proactive key delivery in detail.

A. System Concept

The IEEE 802.11i authentication process can be summarised into two phases[1]: EAP-TLS authentication between MN and the AS and four-way handshake for mutual authentication between MN and AP. Typically, the EAP-TLS introduces a long delay because of the number of exchanged messages, and particularly long round trip time (RTT) between the MN and the AS. This delay can be worse if the MN visits a foreign domain, far away from its home AS. In such scenarios, the foreign domain's AS needs to refer to the MN's home AS to obtain MN's authentication information. Therefore, the EAP-TLS is desirable to be optimised as follows.

The MN performs a full EAP-TLS for the first authentication with a domain. However, this full EAP-TLS will not produce one PMK, but a list of PMKs at both the MN and AS. In subsequent re-authentications within the domain due to handovers, the AS will proactively deliver PMKs to candidate APs. Those candidate APs are identified during the cycle of scanning-to-Context Transfer from the scheme of proactive Context Transfer and Forced Handover [7][8]. The MN and the AS need to agree on a method of key selection from the list. For example, MN uses a list index to indicate PMK associated with a particular candidate AP.

In summary, by combining Forced Handover and Proactive Context Transfer we can reduce the overheads of the EAP-TLS authentication phase upon handovers. This comes at the expense of the complexity of using a PMK list at MN and AS (as opposed to a new PMK each authentication) and, as with any handover prediction technique, the overheads incurred when a prediction fails. In the next section, we will describe the process of proactive key delivery in the authentication with the domain.

B. Process of Proactive Key Delivery

Assuming that the MN successfully performs the first authentication with the domain (i.e. including full EAP-TLS

[1] We do not include the Group Key Delivery as this phase is optional in the 802.11i framework.

authentication and four-way handshake), the process of proactive key delivery in the subsequent authentication is described below. This process is derived from the scheme of proactive Context Transfer and Forced Handover with some detail extensions for the authentication service.

1. The MN starts scanning cycles when the current SNR drops below the threshold SNR_{CST} (box 1 in Figure 4), and estimation of T_{UH} until at least one AP satisfies (T_{UH} < T_{SI}) (box 3 in Figure 4). Recall from Section II.C, (T_{UH} < T_{SI}) means that the current scanning cycle is identified as scanning-to-Context Transfer. This is the best time for MN to initialise the Context Transfer process. To begin with, the MN collects the MAC address of all candidate APs, and send them in a CARD Request message.
2. Upon reception of the CARD Request message, the current AR starts the CARD operation that solves address mapping between MAC address and IP address of all candidate APs (see [15] for details of two schemes mapping MAC address to IP address). Then, the current AR informs the AS about list of candidate APs via a Context Transfer Data message.
3. The AS delivers PMKs to every candidate AP via EAP-Success message, and then notifies the current AR about completion of key delivery (via Context Transfer Data Reply).
4. At the next scanning cycle (box 4 in Figure 4), the MN is forced to perform handover to one of candidate APs. As a part of the handover process, for authentication, the MN just needs to perform **four-way handshake** as the new AP already has the PMK. In other words, there is no need to perform EAP-TLS authentication to generate the PMK.
5. Finally, if the inter-AP handover results in an inter-AR handover, the MN will perform Mobile IP Registration (box 5 in Figure 4), as specified in [3].

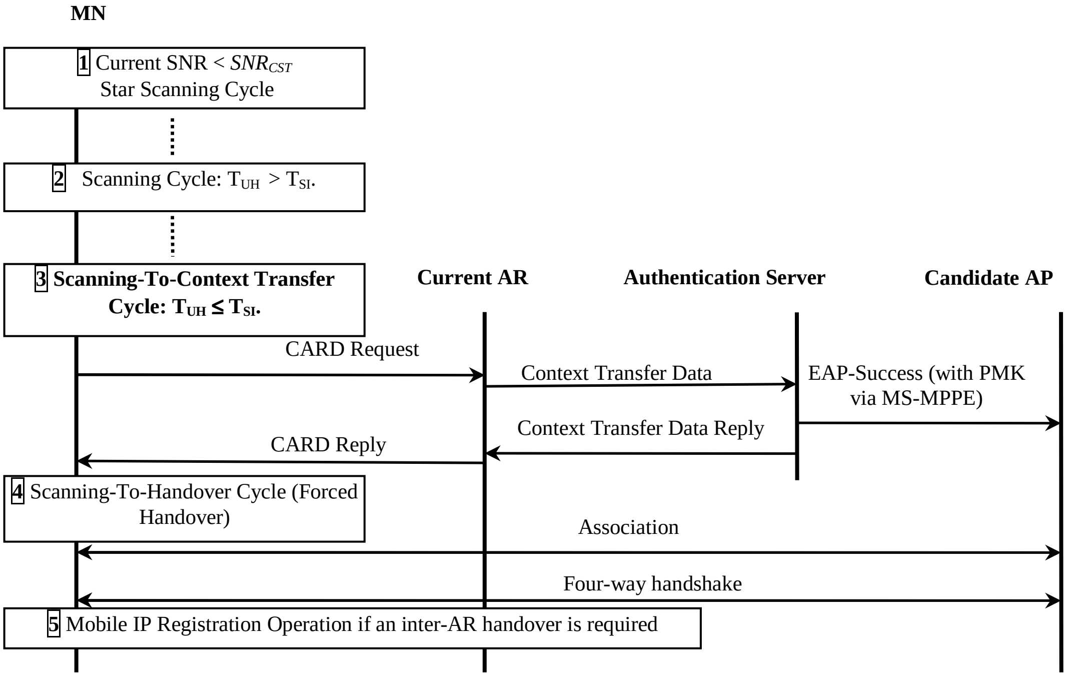
MN
1 Current SNR < SNR_{CST}
Star Scanning Cycle
2 Scanning Cycle: $T_{UH} > T_{SI}$.
3 Scanning-To-Context Transfer Cycle: $T_{UH} \leq T_{SI}$.
Current AR
Authentication Server
Candidate AP
CARD Request
Context Transfer Data
EAP-Success (with PMK via MS-MPPE)
Context Transfer Data Reply
CARD Reply
4 Scanning-To-Handover Cycle (Forced Handover)
Association
Four-way handshake
5 Mobile IP Registration Operation if an inter-AR handover is required

Figure 4 Process of Proactive Key Delivery

IV. Performance analysis

In this section we present a simple performance analysis of the proactive key delivery scheme in terms of authentication delay and bandwidth consumption.

For the authentication delay, we use the following notations T_W – transmission time over a WLAN link; T_L – transmission time over wire-line part between authentication server and AP; T_S – processing time of a message at authentication server; T_{AP} – processing time of a message at AP; T_{MN} – processing time of a message at MN.

From the timing diagram in Figure 3, the delay of EAP-TLS is calculated as follows

$$T_{EAP\_TLS} = 10T_W + 10T_L + 5T_S + 5T_{MN} + 2T_{AP} \qquad (3)$$

The delay of the four-way handshake is defined from the timing diagram in Figure 3

$$T_{4ways} = 4T_W + 2T_{MN} + 2T_{AP} \qquad (4)$$

Therefore, the delay of full authentication is

$$\begin{aligned} T_{full} &= T_{EAP\_TLS} + T_{4ways} \\ &= 14T_W + 10T_L + 5T_S + 7T_{MN} + 4T_{AP} \end{aligned} \quad (5)$$

Recall that the delay of optimized authentication (i.e. authentication with proactive key delivery) is T_{4ways} Comparing T_{full} and T_{4ways}, it is easily to see that the optimized authentication delay T_{4ways} is significantly less than the full authentication delay because the proactive key delivery eliminates processing time at the authentication server (T_S), and reduces number of transmissions over a WLAN link. We emphasize the processing time at the authentication server, neither MN nor AP, because the authentication server is typically responsible for a large number of users. Also, the transmission time over wire-line part (T_L) is incomparable to the transmission time over a WLAN link (T_W) as T_L is quite small within an administrative domain, and T_W may be quite significant due to bandwidth limit and back-off algorithm over WLAN link.

For illustration purpose, we present numerical examples in Figure 5 with assumptions of T_{AP} = 20 ms, T_{MN} = 1ms, T_L = 1 ms. As can be seen from the graph, the proactive key delivery reduces significantly authentication delay, particularly when the authentication server is offered high load (i.e. long processing time T_S).

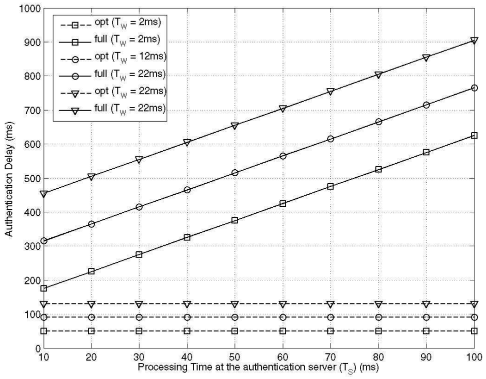

Figure 5 Delays of full and optimised authentications

We also investigated how the proposal reduces bandwidth consumption. For the further discussion, the following notations are used: b_L – bandwidth consumption for one message transmission over wire-line part, b_W – bandwidth consumption for one message transmission over a WLAN link, n - number of handovers the MN performs within an administrative domain, and n_{AP} – average number of candidate APs. In this analysis we assume all messages contribute an equal amount of overhead. Although this is not true, most of the messages are of similar size and for this initial analysis it gives a reasonable estimate of the savings.

From Eq. (5), the bandwidth consumption for the full authentication is

$$b_{full} = (10b_L + 14b_W)n$$

The bandwidth consumption for the optimized authentication is spent on CARD (2 messages over WLAN link), CTP (2 messages over wire-line), EAP-Success messages (1 x n_{AP} messages over wire-line), and the four-handshake messages (see Figure 3):

$$b_{opt} = (10b_L + 14b_W) + [(2 + n_{AP})b_L + 6b_W](n-1)$$

Therefore, reduction of bandwidth consumption is

$$r = \frac{b_{full} - b_{opt}}{b_{full}} = \frac{(n-1)[(8-n_{AP})b_L + 8b_W]}{n(10b_L + 14b_W)} \quad (6)$$

We derive upper bound of reduction r_{upper} as followings. Intuitively, wireless bandwidth is considered more “expensive” than wire-line bandwidth. However, it is also difficult to determine a quantitative comparison between those types of bandwidth. If equality between them is assumed (i.e. $b_W = b_L$ in Eq. (6)), and recall that $n_{AP} \geq 1$, the equality bound of reduction will be

$$r_e = \frac{n-1}{n}\frac{16-n_{AP}}{24} \leq \frac{5}{8}\frac{n-1}{n} = r_{upper}$$

Similarly, we derive the lower bound of reduction as following

$$\begin{aligned} r &= \frac{n-1}{n}\left(\frac{8b_L + 8b_W}{10b_L + 14b_W} - \frac{n_{AP}b_L}{10b_L + 14b_W}\right) \\ &= \frac{n-1}{n}\left(\frac{4}{7} + \frac{b_L\left(\frac{16}{7} - n_{AP}\right)}{10b_L + 14b_W}\right) > \frac{4}{7}\frac{n-1}{n} = r_{lower\_2} \end{aligned}$$

where r_{lower_2} is the lower bound of reduction in the case n_{AP} ≤2. As n_{AP} increases, the lower bound of reduction will decrease. For example, in the case n_{AP} =3, the lower bound of reduction is defined as follows:

$$\begin{aligned} r &= \frac{n-1}{n}\left(\frac{5b_L + 7b_W}{10b_L + 14b_W} + \frac{b_W}{10b_L + 14b_W}\right) \\ &= \frac{n-1}{n}\left(\frac{1}{2} + \frac{b_W}{10b_L + 14b_W}\right) > \frac{1}{2}\frac{n-1}{n} = r_{lower\_3} \end{aligned}$$

Typically, there is very low probability of n_{AP} > 3. For example, the simulation in [7] and [8] showed that the probabilities of having one candidate AP and two candidate APs are at least 95% and 1% respectively. Therefore, it is quite reasonable to assume that n_{AP} ≤ 2. Therefore, the reduction of bandwidth consumption is realistically between the equality bound and lower bounds as

$$r_{lower\_2} < r < r_{upper}$$

Figure 6 shows three bounds against number of handovers (n) the MN performs within an administrative domain. In the realistic case (i.e. $r_{lower\_2} < r < r_{upper}$), it is clear that significant savings on bandwidth consumption from 30% up to 55% can be achieved in the line of n increasing from 2 up to more than 10.

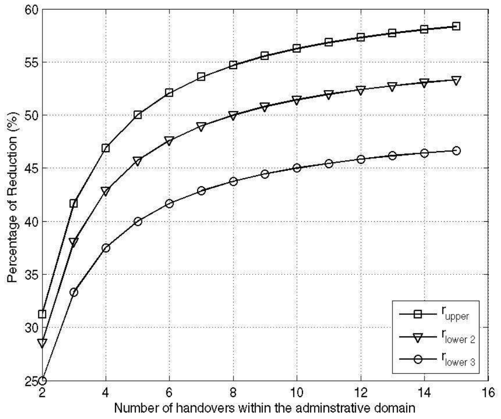

Figure 6 Bounds of Reduction on Bandwidth Consumption.

V. CONLUSION & FUTURE RESEARCH

In this paper, we present a proposal of proactive key delivery to improve re-authentication in WLAN-based access networks. The proposal optimised the EAP-TLS phase of the 802.11i framework by creating multiple PMKs at the first authentication with the administrative domain, and proactively delivering PMKs to candidate APs in subsequent re-authentications. Those candidate APs are identified through the scheme of proactive CT and FH one scanning cycle before the handover moment. The analysis showed that the authentication delay is much shorter and bandwidth consumption is much less (bandwidth saving from 30% up to 55%) thanks to this scheme.

A number of questions need to be addressed in future investigations. An analysis is required to make sure that the scheme provides security at the same level as the full 802.11i framework. Intuitively it should, because we still use PMKs generated by the AS and MN. The list of PMKs also requires investigation, in particular how its size impacts on the implementation of 802.11i and Proactive Context Transfer. Finally, we will investigate the implementation feasibility, for example, in modifications to existing 802.11i framework, and dealing with failure of PMK delivery.

REFERENCE

[1] A. Mishra, M. Shin and W.A. Arbaugh, “Pro-active Key Distribution using Neighbour Graphs,” *IEEE Wireless Comm. Magazine*, Feb. 2004.

[2] B. Aboba, D. Simon, “PPP EAP TLS Authentication Protocol,” RFC 2716, IETF, October 1999.

[3] C. Perkins (editor), “IP Mobility Support for IP v4,” RFC 3320, IETF, Jan 2002.

[4] C. Rigney et al, “Remote Authentication Dial In User Service (RADIUS),” RFC 2865, June 2000.

[5] C. Rigney, W. Willats, and P. Calhoun, “RADIUS Extensions,” RFC 2869, IETF, June 2000.

[6] Cisco Systems Inc., “Cisco AVVID Wireless LAN Design: Solution Reference Network Design”, 2003.

[7] H. Duong, A. Dadej and S. Gordon, “Proactive Context Transfer in WLAN-based Access Networks,” in *Proc. of the 2nd ACM WMASH pp.61-70* , Oct 2004.

[8] H. Duong, A. Dadej, and S. Gordon, “Proactive Context Transfer and Forced Handover in WLAN-based Access Networks”, *ACM Mobile Computing and Communication Review vol.9 num 3,* July 2005.

[9] IEEE, “Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security,” IEEE Std 802.11i/D3.0, Nov 2002

[10] IEEE, “Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” ANSI/IEEE Std 802.11, 1999 Edition.

[11] IEEE, “Standards for local and metropolitan area networks: Standard for port based network access control,” IEEE Standard P802.1X, October 2001.

[12] J. Loughney (editor), “Context Transfer Protocol,” draft-ietf-seamoby-ctp-08.txt, work in progress, IETF, Jan 2004.

[13] L. Blunk and J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP),” RFC 2284, March 1998.

[14] Lucent Technologies Inc., “Roaming with WaveLAN/IEEE 802.11,” Tech. Rep. WaveLAN Technical Bulletin 021/A, Dec 1998.

[15] M. Liebsch, et al., “Candidate Access Router Discovery,” draft-ietf-seamoby-card-protocol-05.txt, work in progress, IETF, Nov 2003.

[16] M. S. Bargh et al, “Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LAN,” in *Proc. of the 2nd ACM WMASH 2004*, pp. 51-60, 1st Oct 2004.

[17] S. Pack and Y. Choi, “Fast handoff scheme base on mobility prediction in public wireless LAN systems,” *IEE Proceedings – Comm.*, vol. 151. No 5, pp. 489 - 495, Oct 2004.

[18] T. Dierks and C. Allen, “The TLS Protocol Version 1.0”, RFC 2246, January 1999.

[19] W. A. Arbaugh el at., “Your 802.11 Wireless Network Has No Clothes,” *IEEE Wireless Comm. Magazine*, pp. 44-51, Dec 2002.