Key Distribution Mechanisms for IEEE 802.21-Assisted Wireless Heterogeneous Networks

F. Bernal-Hidalgo, R. Marin-Lopez, and A. F. Gómez-Skarmeta

Faculty of Computer Science, Dept. Information and Communications Engineering, University of Murcia
{fbernal,rafa,skarmeta}@um.es

Abstract. In recent years there has been a significant growth in the deployment of heterogeneous wireless technologies. Due to its diversity, new multi-interface terminals have appeared and pose new challenges to mobility management and security in wireless networks. In order to achieve a solution to these new challenges several standardisation groups are working to provide solutions that enable a seamless handoff in heterogeneous wireless networks by reducing the latency to obtain network access. In particular, the standardisation task group IEEE 802.21a is studying new media-independent services that allow a secure handoff process as well as mechanisms to reduce the latency during network access control after a mobile handoff. In this article, we analyse, three well-known key distribution mechanisms, in the context of IEEE 802.21a, for secure handover and how these mechanisms can help to reduce the network access time after a handoff in IEEE 802.21-assisted networks.

1 Introduction

In the last years the evolution of data networks and wireless devices have risen dramatically. Moreover, the proliferation of wireless access technologies implies that network subscribers can connect anywhere at any time using real time (e.g. voice calls or video streaming) applications that usually require high performance networks. For that reason, nowadays, several devices support different wireless technologies such as WiFi [1], third generation wireless connectivity (3G), or WiMAX. Due to this increasing diversity, operators must facilitate access to multiple wireless technologies through a single device.

Supporting handoff by avoiding loss of connectivity is the key enabling operation for seamless roaming and high-quality content delivery. Moreover, inter-technology handoff must be supported due to the growing network heterogeneity. An important factor that notably affects the provision of a seamless handoff between heterogeneous wireless technologies is the network access authentication and authorisation processes, by which operators control their subscribers, when they try to access the network service.

K. Pentikousis et al. (Eds.): MONAMI 2010, LNICST 68, pp. 123–134, 2011.

Different standardisation bodies are providing solutions to handle these kinds of problems in heterogeneous wireless networks. One general approach is the so-called SRHO. In this mechanism, a multi-interface terminal only transmits, at any given time, through a single radio interface during the handoff process. By means of SRHO, most of the processes (e.g. association, authentication, etc...) required to get network access are performed by using the single radio interface with the network where the mobile is intended to associate in the near future. For example, WiMAX forum [2] is working on a SRHO solution that handles both WiMAX-WiFi and WiFi-WiMAX inter-technology handoffs [3]. Also, 3GPP [4] is working on a Single Radio solution called SRVCC [5] which provides a service continuation between 3GPP and 3GPP2 [6]. It is also expected that IP-based 3GPP services will be provided through various access technologies, including existing broadband radio access standards like WiMAX.

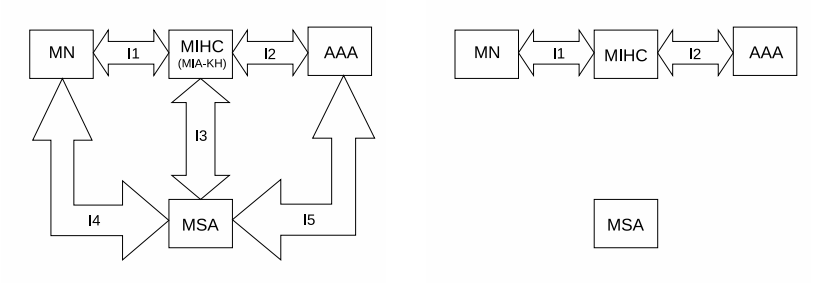
Additionally, IEEE 802.21 [7] standard defines media-access independent mechanisms to facilitate and enable optimisations to improve handoffs between heterogeneous wireless networks. So that, the main aim of this specification is to achieve seamless handoff between heterogeneous technologies. The standard defines all necessary elements required to exchange information, events and commands to facilitate handoff initiation (network discovery and selection process) and handoff preparation (network establishment before the movement). Specifically, there are several tasks groups which are defining new extensions to IEEE 802.21. For example, part of these extensions are being discussed in the IEEE 802.21c task group [8], where some MIH messages are being defined to transport link-layer frames to assist the SRHO mechanisms in WiMAX-WiFi and WiFi-WiMAX handoffs. Moreover, IEEE 802.21a task group [9] is defining mechanisms to further reduce the latency introduced by the authentication and authorisation processes usually required to get network access during the handoff process (working item #1); and security extensions to protect 802.21 messages (working item #2).

In particular, our contribution analyses and describes in detail the integration of three general and well-known key distribution mechanisms in the context of IEEE 802.21-assisted wireless networks in order to provide a secure handover and reduce the latency to get network access after the mobile handoff process. That is, the analysis which we describe in this article is focused in IEEE 802.21a working item #1.

This article is organised as follows. The section 2 describes the general architecture and specific details about the integration of the three general key distribution mechanisms in IEEE 802.21-assisted wireless networks. In particular, we will describe how to carry out a fast and secure heterogeneous handoff by using these key distribution mechanisms. Moreover, a deployment analysis is provided in section 3. Section 4 provides a performance analysis and shows how the key distribution mechanisms can further reduce the latency in solutions based on SRHO. Finally, section 5 provides some important conclusions and shows some future directions.

Table 1. Summary of used acronyms

Acronym	Definition	Acronym	Definition
SRHO	Single Radio HandOver	SRVCC	single Radio Voice Call Continuity
MIA-KH	Media Independent Authenticator and Key Holder	MSA-KH	Media Specific Authenticator and Key Holder
MN	Mobile Node	MIHC	Media Independent Handover Controller
MS-PMK	Media Specific Pairwise Master Key	MI-PMK	Media Independent Pairwise Master Key
TN-PMK	Tunnel Pairwise Master Key	PSK	Pre-Shared Key



(a) General Architecture

(b) Media Independent Authentication Architecture

Fig. 1. General Media Independent Architecture

2 Key Distribution for Media Independent Handoff

2.1 General Architecture

In the context of IEEE 802.21a, the proposal specified in [12] defines an architecture based on a MIA-KH entity (see Fig.1(a)). In this architecture, this entity controls and interacts with a set of MSA-KHs and facilitates the MN to perform a (proactive) authentication *before* moving to a *target* MSA-KH. Nevertheless, in order to complete the network access process, a key distribution mechanism is required to distribute key material to the target MSA-KH in order to establish a security association between the MN and the MSA-KH. If this key distribution process is carried out before the handoff, it will cause a reduction of (and in some cases, even eliminate) the authentication process. In general, it is initially assumed that a target MSA-KH will require an authentication based on the EAP [10] (unless some optimised key distribution is deployed), which has been recognised as a very flexible authentication protocol and used in multiple wireless technologies (e.g. WiFi or WiMAX) but is not as appropriate for authentication in mobile networks [11].

However, how key distribution is performed has not yet been deeply discussed in the context of the proposal [12]. Thus, in our contribution, we analyse and describe the integration of three well-known key distribution mechanisms but take into account the MIA-KH/MSA-KH architecture described above. We have considered these key distribution mechanisms as MIH services provided by the MIA-KH to the MN. According to this approach, we consider that the MN should

be authenticated and authorised to use these services. As such, we believe that MIA-KH can be such an entity since it allows a (proactive) media-independent authentication. However, we consider that in order to embrace the concept of MIH service, a more generic name is required, as not only media-independent authentication, but also key distribution services are provided by that entity. Therefore, we have renamed MIA-KH to MIHC and its functionality has been updated to provide both secure MIH signalling and help to reduce the network access time by providing different key distribution services: push, reactive pull and proactive pull key distribution.

Thus, the use of the MIHC entity has two main goals: one is to authenticate and authorise the use of the MIH services and the second is to assist the proper execution of them.

Table 2. Summary of External Interfaces for Media Independent Authentication and Key Distribution

Interface	Functionality
I1	It is used for performing the Media Independent Authentication, Push and Proactive Pull Key Dist. mechanisms. It is in charge of transporting MIH signalling, all required information for the key dist. method and the authentication protocol for media-independent authentication
I2	It is used to transport the authentication protocol to the MN's home domain in order to perform the authentication (e.g. AAA protocol)
I3	It enables, in Push Key Distribution, the MIHC to install a MS-PMK in the target MSA-KH. Moreover, in Proactive Pull Key Distribution, it transports the target technology level two frames to the MSA-KH
I4	It is used to communicate the MN with the MSA-KH
I5	It is used by the target MSA-KH to communicate with the AAA server

In order to achieve these goals, entities needs to communicate through several interfaces. Table 2 shows a summary of the interfaces used by each entity depending on the key distribution method used and the interfaces required for the media-independent authentication.

2.2 Media Independent Authentication Process

Before providing any MIH key distribution service, a media-independent authentication (Fig. 1(b)) by using some extensions to the MIH protocol (I1) is required between the MN and MIHC. The media independent authentication is composed by four phases:

1. *Negotiation phase.* Both the MN and the MIHC exchange unprotected MIH messages in order to agree on the type of key distribution mechanism to be used in that session and other related parameters.
2. *Media-Independent Authentication phase.* The MN and MIHC authenticate each other by using MIH signaling (I1) in order to get access to the key

distribution services. Moreover, MIHC may contact a backed authentication server (e.g. AAA server) to verify MN's credentials by using I2. In general, this media-independent authentication will be performed with the MIHC before the MN moves to a target MSA-KH under the control of the MIHC, in a so-called *proactive media-independent authentication*. In this case, we refer to the MIHC as *Candidate MIHC*. After performing the (proactive) authentication, key material will be shared between the MN and the MIHC, so that the rest of the MIH communication (I1) can be protected using this key material. This shared key, which is used as a root key for further key derivation, is a so-called *Media Independent Pairwise Master Key* (MI-PMK). At the end, the negotiated parameters in the negotiation phase are confirmed and an authentication session is established. For the purpose of this article, we assume that EAP is used as the authentication protocol since it provides a flexible way [10] to perform such authentication process.

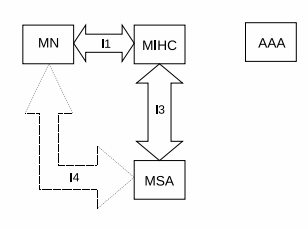
3. *Authenticated/Authorised phase*. In this phase, the MN is already authenticated and authorised to use the key distribution services provided by the MIHC.
4. *Finalisation phase*. When either the MN or the MIHC desire to finish the authentication session, they send protected MIH messages in order to release the MN's state related to the provided MIH services.

Once the MN is authenticated, we propose the use of three types of key distribution mechanisms (Push, Reactive Pull and Proactive Pull key distribution) which bring some interesting advantages (but also some associated disadvantages) to reduce network access latency as we describe in the following sections.

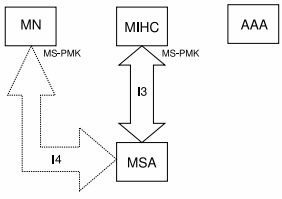
2.3 Push Key Distribution

In the *Push Key Distribution* mechanism (Fig. 2(a)), the MIHC pushes a key into the target MSA-KH on the a MN's request (*mobile-initiated process*) or some decision made by the MIHC itself (*network-initiated process*). The distribution process must be signaled by using protected MIH messages (I1) before the handoff to the target MSA-KH. Otherwise, an attacker could initiate the process. Then, the MN and MIHC will derive from the MI-PMK a specific MS-PMK for the target MSA-KH. To complete the process, the MIHC will push the MS-PMK into the target MSA-KH (under the control of the MIHC) by using interface I3.

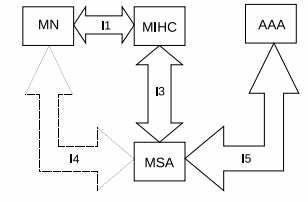
Once the key has been installed, the MN can perform the handoff to the target MSA-KH, and establish the link-layer association and the security association to protect link-layer frames using I4. In general, the MN can pro-actively request pushing a new key in another MSA-KH under the control of the MIHC. Thus, using the key hierarchy derived from the MI-PMK, it is possible to access different MSA-KH without performing an EAP authentication each time the MN handoffs to a new MSA-KH under the same MIHC. So, the network access time after handoff can be reduced considerably.



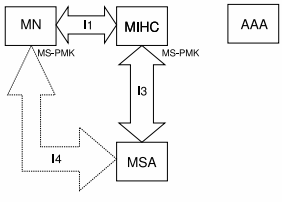
(a) Push Key Distribution



(b) Reactive Pull Key Distribution



(c) Regular Proactive Pull Key Distribution



(d) Optimized Proactive Pull Key Distribution

Fig. 2. Key Distribution Mechanisms

2.4 Reactive Pull Key Distribution

The *Reactive Pull Key Distribution* mechanism (Fig. 2(b)) operates with the assumption that the MN and MIHC shares a symmetric key MS-PMK derived from the MI-PMK. In this sense, the MS-PMK should be considered as a *mid-term* credential shared between MN and MIHC for this type of key distribution. The MS-PMK will be used in a media-specific EAP re-authentication process based on an EAP method or mechanism (e.g. ERP [13]) that uses symmetric keys. This EAP re-authentication will happen *after* the MN moves to the target MSA-KH. In this EAP authentication, MIHC will act as EAP/AAA server and the target MSA-KH as an EAP authenticator.

Then, as a consequence of the media-specific EAP re-authentication which is performed by means of interface I4 and I3, an MSK is derived for the MSA-KH by the MIHC acting as AAA server. This MSK will be used to establish the security association between the MN and the target MSA-KH.

In order to achieve improvement with this key distribution mechanism, we propose the use of a temporal (NAI) [14] which must be provided for the MN. The temporal NAI can be provided during the media-independent authentication with the MIHC by means of interface I1 (Fig.1(b)). In general, this temporal NAI will have the format $user@mihc-realm$ where $mihc-realm$ can be the Fully Qualified Named (FQDN) of the MIHC. With this information, the target MSA-KH and/or the AAA infrastructure behind, can route the authentication and authorization (AAA) information to the MIHC during the media-specific

EAP re-authentication. The key aspect to reducing time with this type of key distribution is that the MIHC is assumed to be very near to the target MSA-KH so the latency between this entity and the MIHC is low.

2.5 Proactive Pull Key Distribution

The *Proactive Pull Key Distribution* mechanism allows media-specific EAP authentication without the need of the MN being directly connected to the wireless link of the target MSA-KH. To carry out this mechanism, it is necessary to transport link-layer authentication frames for the corresponding target MSA-KH wireless technology over a media-independent tunnel between the MN and MIHC (I1); and to convey those link-layer frames between the MIHC to the target MSA-KH by means of another tunnel (I3). In this way, after successful completion of the proactive media-specific authentication, a MSK will be pulled by the target MSA-KH as happens in a typical EAP authentication.

We have considered two main cases with this mechanism: The *regular Proactive Pull Key Distribution* (Fig.2(c)) and the *optimized Proactive Pull Key Distribution* (Fig 2(d)). In the former, the MN uses its NAI (e.g. $user@home-domain$) with the home domain (where the MN is subscribed to) in the proactive media-specific EAP authentication with the target MSA-KH. In this case, the authentication and authorisation process will be routed to the AAA server in the MN's home domain. In the latter, it is assumed that a MS-PMK is shared between the MN and MIHC as happens in Reactive Pull Key Distribution. Thus, it is also necessary to use a temporary NAI for EAP re-authentication purposes with the same format described in section 2.4, in order to forward the information to the corresponding MIHC (acting as a local AAA server).

Finally, it is worth noting that in order to implement the media-independent tunnel between MN and MIHC, we have considered two options: 1) carrying link-layer authentication frames over protected MIH signaling (this option is being considered on IEEE 802.21c as well); or 2) by the establishment of a dynamic secure IP tunnel (e.g. IKEv2) between the mobile node and the MIHC. This first option uses the interface I1 to transport link-layer authentication frames and the second option uses I1 to request the establishment of this secure IP tunnel. In the second option, the MN and MIHC will derive a pre-shared key (TN-PMK) obtained from key hierarchy rooted in the MI-PMK. With that key the secure IP tunnel will be established (e.g. IKEv2 with PSK authentication where the TN-PMK will be used as PSK).

From our point of view, we consider the second option as a better option because it separates MIH signaling from the tasks purely assigned to tunneling purposes.

3 Deployment Implications

In this section we describe the most important implications (advantages and disadvantages) that must be taken into account in the deployment of the three key distribution mechanisms that we have described in the previous sections.

For example, to use the *Push Key Distribution* mechanism the target MSA-KH must provide an implementation of interface (I3) in order to allow MIHC to push a key into the MSA-KH. Thus, to the best of our knowledge, no wireless technologies have standardised any interface that allows an external entity to push a key. To install a key, SNMP [15] could be used, but several changes must be carried out to do this. Conversely, the operation of the *Reactive Pull Key Distribution* does not need any change in existing wireless standards and, therefore, in the existing deployed target MSA-KHs. However, in the *Reactive Pull Key Distribution*, one possible deployment issue is that the MIHC also needs to act as AAA server in this process and there is no current entity nowadays which acts as an AAA client (for media independent authentication) and as a AAA server at the same time.

Additionally, the use of the (regular or optimized) *Proactive Pull Key Distribution* mechanism requires that the target MSA-KHs accepts wireless link-layer authentication frames over a wired link (the same issue is raised in single-radio handover case). Furthermore, a protocol to transport these frames from the MIHC to the target MSA-KH is required. Moreover, for the specific case of the optimized Proactive Pull Key Distribution, the MIHC must act again as AAA server in the proactive media-specific EAP re-authentication.

Also, obviously, MIHC functionality must be deployed on the existing networks. There are several alternatives. The first one is that the MIHC entity could be co-located with other existing entities (e.g. local AAA server). In this case, the software for these entities must be modified in order to support the new functionalities provided by the MIHC. In the second alternative, the MIHC could be a separate entity. In this case, the new entity must be deployed and connected with the rest of the network entities. Taking into account that other standardisation work considers including new entities and functionalities (e.g. WiMAX and WiFi Signal Forwarding Functions [3]) the first alternative seems the most promising option.

Finally, on the MN side, mobile terminals must be updated to support MIH protocol, manage the new key hierarchy and implement the different interfaces needed to support these key distribution methods.

4 Remarks on Performance

Nowadays, there is no existing implementation of these key distribution mechanisms in the context of IEEE 802.21-assisted wireless networks. So, this makes it difficult to obtain real experimental values in order to evaluate the key distribution mechanisms. For that reason, we have used real measurements taken from [16] [17] [18], where simulations and real scenarios have been used, to compute an approximate authentication delay, and to provide a rough analysis on how these key distribution mechanisms provide benefits during handoffs. Furthermore, using these mechanisms, other proposals (e.g. SRHO, IEEE 802.21c) can also improve their performance.

The following notation is used. T_{assoc} and T_{re_assoc} represents the time of performing a complete association and re-association *after* the attachment to the target MSA-KH, respectively. Note that, in general $T_{assoc} >\approx T_{re\_assoc}$ because performing a re-association process usually involves less messages. For example, if we consider IEEE 802.11, we assume that T_{assoc} includes 3 roundtrips [1]; whereas T_{re_assoc} only includes one roundtrip, as happens in IEEE 802.11r [19]. In [18] T_{assoc} implies a time of $\approx 20ms$ so, taking into account [18] and [19] we will roughly say a time of $6-7ms$ for T_{re_assoc}.

$T_{ms-auth}$ refers to the time consumed in carrying out a media-specific full EAP authentication between the MN and the MSA-KH that involves the MN's home domain. Based on [16] we can assume that $T_{ms-auth}$ is $\approx 600ms$ (in roaming case). $T_{ms-fast\_reauth}$ refers to the media-specific EAP re-authentication time without the need to contact with the MN's home domain but with the contact with the MIHC acting as AAA server. $T_{ms-fast\_reauth}$ could take $\approx 100ms$ according to [17]. Therefore, as [16] and [17] show, the assumption that $T_{ms-auth} >> T_{ms-fast\_reauth}$ is feasible. T_{sap} denotes the time of performing a secure association protocol (e.g. 4-way handshake in WiFi networks). Based on the measurements in [16] T_{sap} may take $\approx 10ms$. T_{push_key} refers to the time involved in contact with the target MSA-KH to push the corresponding key. Based on [16] we can assume a time of $\approx 10ms$. $T_{MIH_{push}}$ will refer to the time involved in the signaling required to indicate to the MIHC to install a key. Although there is no experimental data, we expect that this time will involve one exchange, as T_{push_key}. So, we could roughly assume that $T_{MIH_{push}}$ may also take $\approx 10ms$.

Taking into account these assumptions, when a MN moves to a target MSA-KH and no improvement is provided to reduce the network access delay, the latency to get network access through that MSA-KH can be computed in a very general way as:

$$T_{networkaccess_{total}} = T_{assoc} + T_{ms-auth} + T_{sap}$$

The table 3 shows the times only applicable to the different key distribution mechanisms described above. It shows two different time components: the time spent before the MN moves to the target MSA-KH (*Handoff Preparation Time*) and the time spent after the MN moves to the target MSA-KH (*Handoff Execution Time*). To obtain a rough estimation about the benefit of the performance of the three key distribution mechanisms adapted to the IEEE 802.21 context, we also assume that the MN has already performed the media-independent authentication with MIHC.

For this general analysis, we assume that $T_{MIH_{push}} + T_{push\_key} <\approx T_{ms-fast\_reauth}$. The reason for this assumption is that, $T_{MIH_{push}}$ involves one roundtrip between the MN and MIHC and T_{push_key} one roundtrip between the MIHC and the target MSA-KH. In $T_{ms-fast\_reauth}$ a similar number of roundtrips are required. For example, that happens when using ERP [13], since it is the most optimised and fast re-authentication solution defined in the IETF,

Table 3. Computed times for key distribution mechanism

Mechanism	Handoff Prep. Time	Handoff Exec. Time
Push	$T_{MIH_{push}} + T_{push\_key}$	$T_{assoc} + T_{sap}$
Reactive Pull		$T_{assoc} + T_{ms-fast\_reauth} + T_{sap}$
Proactive Pull	$T_{ms-auth}$	$T_{assoc} + T_{sap}$
Proactive Pull (optimized)	$T_{ms-fast\_reauth}$	$T_{assoc} + T_{sap}$

Table 4. Times when applying key distribution mechanisms to SRHO

Mechanism	Handover Prep. Time	Handover Exec. Time
SRHO	$T_{assoc} + T_{ms-auth} + T_{sap}$	T_{re_assoc}
SRHO+Push Key Dist.	$((T_{MIH_{push}} + T_{push\_key}) << T_{ms-auth}) + T_{assoc} + T_{sap}$	T_{re_assoc}
SRHO+ Proactive Pull (opt.)	$T_{assoc} + ((T_{ms-fast\_reauth}) << T_{ms-auth}) + T_{sap}$	T_{re_assoc}

where, in the best case, only one roundtrip is required. However ERP (or other authentication protocols) may require, in some specific cases, some additional message to complete a fast re-authentication process.

Taking into account these assumptions, we may observe that the Push Key Distribution will (potentially) reduce the network access time to only $T_{assoc} + T_{sap}$ when the MN attaches the target MSA-KH in each inter-MSA-KH handoff under the same MIHC. Although this equals the value of others key distribution mechanisms (proactive and optimized proactive pull key distribution), it has low latency at handoff preparation which is an advantage when the MN moves quickly to a new target MSA-KH under the same MIHC[1]. However, *Push Key Distribution* has some important deployment issues as discussed in section 3.

As we may also observe from table 3, the *Reactive Pull Key Distribution* will contribute with additional latency to network access control process after the MN attaches the target MSA-KH and will exhibit worse performance due to the MN fast re-authentication ($T_{ms-fast\_reauth}$) being carried out *after* MN moves to the target MSA-KH; this implies an increment in the latency with respect to other key distribution mechanisms but it actually represents a trade-off between easier deployment (see section 3) and fast network access.

It is also very important to note that some of the key distribution mechanisms could be used to minimise the handoff preparation time in SRHO process discussed in IEEE 802.21c. This is important, as commented before, if the MN moves quickly between MSA-KHs. In this manner, SRHO combined with either Push or Optimised Proactive Pull Key Distribution mechanisms can considerably reduce the SRHO handover preparation time and improve its benefits. Specifically, table 4 shows the combination of both methods and the time reduction achieved in SRHO. The first row in the table shows the general times involved in a traditional SRHO process. The rest of rows show how the use of the key distribution mechanisms can help the SRHO process. Basically, following the same assumptions as before, SRHO + Push Key Distribution can obtain better

[1] If a MN moves quickly the handoff preparation could not finish and not improvement would be achieved.

performance for the same reason as we already described. That is, *Push Key Distribution* takes a reduced time including preparation and execution handoff. So, this combination minimizes the problem of a MN moving to a target MSA-KH without completing the handoff preparation process.

5 Conclusions

In this work, we have analysed and described in detail how to integrate three general and well-known key distribution mechanisms in the context of IEEE 802.21-assisted heterogeneous wireless networks. The general architecture is based on an entity that we have called MIHC, which is an extension of the architecture described in [12]. The interfaces and the entities involved in the MIHC architecture have been defined and described, as well as, each key distribution mechanism. We have also discussed several deployment issues that must be taken into account in the real deployment of each key distribution mechanism. Finally, a general performance discussion about how the general and well-known key distribution mechanisms integrated in IEEE 802.21, can help to reduce the network access latency during handoff.

As future goals, we are now focused not only on the definition of the specific MIH messages for supporting the key distribution mechanisms introduced but also the implementation, based on ODTONE [20], of the mechanisms described in this manuscript to obtain experimental results. In continuation, with the specific values obtained during our experiments, we will perform simulations to observe the advantages and disadvantages of the described key distribution mechanisms, considering different types of use cases, wireless technologies and number of mobile nodes.

Acknowledgements

This work has been supported by the Funding Program for Research Groups of Excellence with code 04552/GERM/06 granted by the Seneca Foundation. Thanks also to the project CICYT TIN2008-06441-C02-02 which has also supported this work.

References

1. IEEE 802.11, `http://www.ieee802.org/11/`
2. WiMAX-3GPP Interworking WMF-T37-002-R010v3 (January 2008)
3. WiFi-WiMAX Interworking DRAFT, `https://mentor.ieee.org/802.21/dcn/10/21-10-0014-00-0000-wifi-wimax-iwk-spec.pdf`
4. 3GPP 3rd Generation Partnership Project (3GPP), `http://www.3gpp.org/`
5. 3GPP Single Radio Voice Call Continuity (SRVCC) TS 23.216
6. 3GPP 3rd Generation Partnership Project 2(3GPP2), `http://www.3gpp2.org/`
7. IEEE 802.21 Media Independent Handover Working Group, `http://ieee802.org/21/`

8. IEEE 802.21 Optimized Single Radio Handovers PAR and 5C 21-09-0146-05-0000-single-radio-handovers-par-and-5c.doc (November 2009)
9. IEEE Security SG Technical Report 21-08-0172-02-0sec-21-08-0012-02-0sec-mih-security-technical-report.doc (December 2008)
10. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP) RFC 3748 (June 2004)
11. Clancy, T., Nakhjiri, M., Narayanan, V., Dondeti, L.: Handover Key Management and Re-Authentication Problem RFC 5169 (March 2008)
12. IEEE 802.21a Proactive Authentication and MIH Security 21-09-0102-02-0sec-proactive-authentication-and-mih-security.doc (September 2009)
13. Narayanan, V., Dondeti, L.: EAP Extensions for EAP Re-authentication Protocol (ERP). RFC 5296 (August 2008)
14. Aboba, B., Beadles, M., Arkko, J., Eronen, P.: The Network Access Identifier. RFC 4282 (December 2005)
15. Case, J., Fedor, M., Schoffstall, M., Davin, J.: A Simple Network Management Protocol (SNMP) RFC 1157 (May 1990)
16. Lopez, R.M., Dutta, A., Ohba, Y., Schulzrinne, H., Gomez, A.F.: Skarmeta Network-Layer Assisted Mechanism to Optimize Authentication Delay During Handoff in 802.11 Networks mobiquitous, MobiQuitous, pp.1–8 (2007)
17. Marin-Lopez, R., Pereiguez-Garcia, F., Ohba, Y., Bernal-Hidalgo, F., Gomez, A.F.: A Kerberized Architecture for Fast Re-authentication in Heterogeneous Wireless Networks. Mobile Networks & Applications, 1–21 (2010)
18. Machan, P., Wozniak, J.: Simultaneous handover scheme for IEEE 802.11 WLANs with IEEE 802.21 triggers. Springer Science+Business Media (2009)
19. IEEE 802.11r-2008, `http://www.ieee802.org/11/`
20. ODTONE, `http://hng.av.it.pt/projects/odtone`