A New Standard for Securing Media Independent Handover: IEEE 802.21a

Rafa Marin-Lopez, Fernando Bernal-Hidalgo, Subir Das, Lidong Chen, and Yoshihiro Ohba

***Abstract*—When enabling handover between different radio interfaces (e.g., handover from 3G to Wi-Fi), reducing network access authentication latency and securing handover related signaling messages are major challenging problems, amongst many others. The IEEE 802 LAN/MAN Standards committee has recently finished its standardization work in this area by defining the IEEE std 802.21a-2012^{TM}. The mechanisms introduced in this standard are aimed to protect the IEEE std 802.21-2008^{TM} messages and services and to reduce handover latency by introducing the concept of proactive authentication. We provide a comprehensive survey of this standard and describe how the defined mechanisms can be used to reduce the overall latency during handover between access networks using heterogenous radio interfaces.**

***Index Terms*—Media Independent Handover, IEEE 802.21, Fast Handover, Security.**

I. Introduction

THE proliferation of smart devices with multiple radio interfaces (e.g., 3G/4G, Wi-Fi, WiMAX) has ushered in a new era of user connectivity to the network. Users would like to be always connected to the Internet with seamless handover experience between different access networks. Thus the traditional model of network connectivity for legacy cell phones with a single cellular interface has completely changed.

Indeed, cellular operators are today experiencing the exponential growth of their network data and are actively looking forward to offloading the bandwidth hungry applications and users to alternate access networks. The availability of radio access technologies (e.g., Wi-Fi, WiMAX) and interoperable standards are making this vision a reality. In recent years several such standards are published, including, but not limited to Mobile IPv6 and Proxy Mobile IPv6 defined in *Internet Engineering Task Force* (IETF); *Local IP Access and Selected IP Traffic Offload* (LIPA-SIPTO) and *Access Network Discovery and Selection Function* (ANDSF) in *3rd Generation Partnership Project* (3GPP); and *Hotspot2.0* in *Wi-Fi Alliance*^{TM} (WFA). Key enabling features include seamless handover techniques, handover policies and pre-authentication or pre-registration. These techniques are necessary to reduce the session handover delay and provide a better user experience.

Rafa Marin-Lopez, and Fernando Bernal-Hidalgo are with the Dept. of Information and Communications Engineering, University of Murcia, Spain; e-mails: rafa@um.es, fbernal@um.es

Subir Das is with Applied Communication Sciences; e-mail: sdas@appcomsci.com

Lidong Chen is with National Institute of Standards and Technology (NIST); e-mail: lily.chen@nist.gov

Yoshihiro Ohba is with Toshiba Corporate R&D; e-mail: yoshihiro.ohba@toshiba.co.jp

Manuscript received ; revised .

While several of these standards were under development, IEEE std 802.21-2008^{TM} [1] was developed to provide a *Media Independent Handover* (MIH) framework to facilitate handover between heterogeneous access networks. The motivation was to provide an abstract layer that can present an uniform view of the lower layers to the higher layers across multiple radio interfaces and thereby facilitate a better user experience.

The new IEEE std 802.21a-2012^{TM} [2] then defines the security extension of MIH framework and mechanisms to minimize the time required for network access authentication during handover. In this article, we provide a comprehensive survey about this recent standard, published in May 2012. Firstly, we provide some background information on IEEE std 802.21-2008^{TM} in Section II. In Sections III and IV, we introduce and analyze the security mechanisms of MIH services which are defined in IEEE std 802.21a-2012^{TM}. In Section V, we discuss some challenges with the current specification and what on-going work is being undertaken. Finally, Section VI concludes the article.

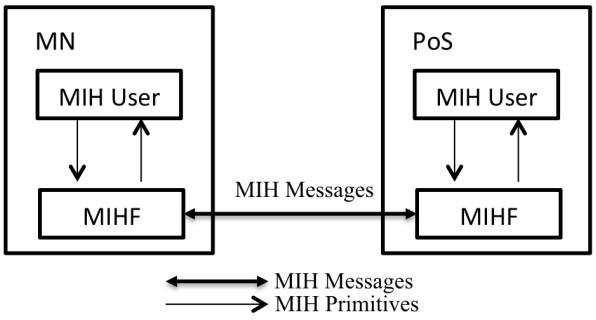
II. Background

In IEEE std 802.21-2008^{TM}, handover is defined as an attempt of a *Mobile Node* (MN) to change its network serving *Point of Attachment* (sPoA) to another *target PoA* (tPoA) (see Figure1(b)). When two PoAs provide the same access technology and are controlled by the same administrative domain, handover is generally achieved by the corresponding link-layer mechanisms (e.g., LTE, IEEE 802.11). Alternatively, when two PoAs are communicating with two different access technologies, handover is supported at the network or higher layers. Several mobility management protocols (e.g., Mobile IP and its variants) provide such capabilities. In general, these protocols may require information about neighboring PoAs before proceeding with the handover.

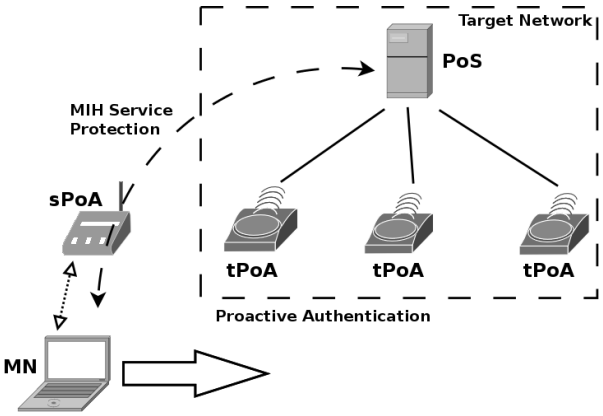
MIH framework defines three media independent services [3] that can help to provide the information to assist the handover: *Information Service* (MIIS); *Event Service* (MIES); and *Command Service* (MICS) through which it provides:

- neighboring network information (e.g., available Wi-Fi networks);
- early indication of link performance (e.g., link going down);
- the ability for the network and the communicating node to control the handover (e.g., move to another network).

The core of this framework is an *MIH Function* (MIHF) that provides services to upper layer protocols known as *MIH*



(a) MIH Functional Model



(b) MIH Deployment Model (with IEEE std 802.21a-2012^{TM} extensions)

Fig. 1. MIH framework

Users (e.g., Mobile IP) (see Figure 1(a)). It defines a set of functions or *primitives* that constitute logical interfaces between the MIHF and other entities, and a protocol that provides remote communication messages between two MIHF peers. The MIH protocol is designed to operate over both a link-layer and a network-layer. Details of this framework and its applicability are specified at [1]. In a practical deployment model, one MIHF peer will reside in a MN and another one is on a network node typically on a network server. This network server is called a *Point of Service* (PoS) that provides remote MIH services to the MN. The *Point of Attachment* (PoA) to the network (e.g., Wi-Fi access point, WiMAX base station...) may be separated from the PoS in typical deployments (see Figure 1(b)).

From a communication perspective, security of remote MIH services is critical. Security is covered by the new IEEE std 802.21a-2012^{TM}, which is the focus of our article. Security solutions for the media independent services are needed in two aspects:

- **MIH Service Protection**. This is to protect MIH messages for all three services defined under MIH framework. The mechanisms to protect these services are presented in Section III.
- **Proactive Authentication**. This is to provide the means by which network access authentication can be executed before a handover is performed to the target network. The techniques for proactive authentication are presented in Section IV.

In other words, IEEE std 802.21a-2012^{TM} not only defines how to secure the access to the MIH services, but also adds new services to the IEEE 802.21 framework which reduce the latency of performing security processes during handover.

All of the security mechanisms are realized in IEEE std 802.21a-2012^{TM} by defining new information elements (IEs) (i.e., the basic data units to carry specific information), new MIH primitives (i.e., internal function calls that constitute an interface with an MIH entity) and new MIH messages (sent between MIH entities).

III. MIH Service Protection

To understand which kind of security mechanisms are needed to protect the MIH service, let us look at the situation when a MN, already connected to the network, wants to access the services provided by a particular PoS. The MN needs to be sure that the PoS is a trusted entity to provide the service. On the other hand, the PoS may provide service only to authenticated and authorized MNs. Thus, a mutual authentication process is required before providing the service. Once the mutual authentication is successfully completed, the MIH exchanges during the access to the service should be protected. Thus, a key establishment procedure between the MN and PoS is also needed to obtain the keys to be used for the protection algorithms.

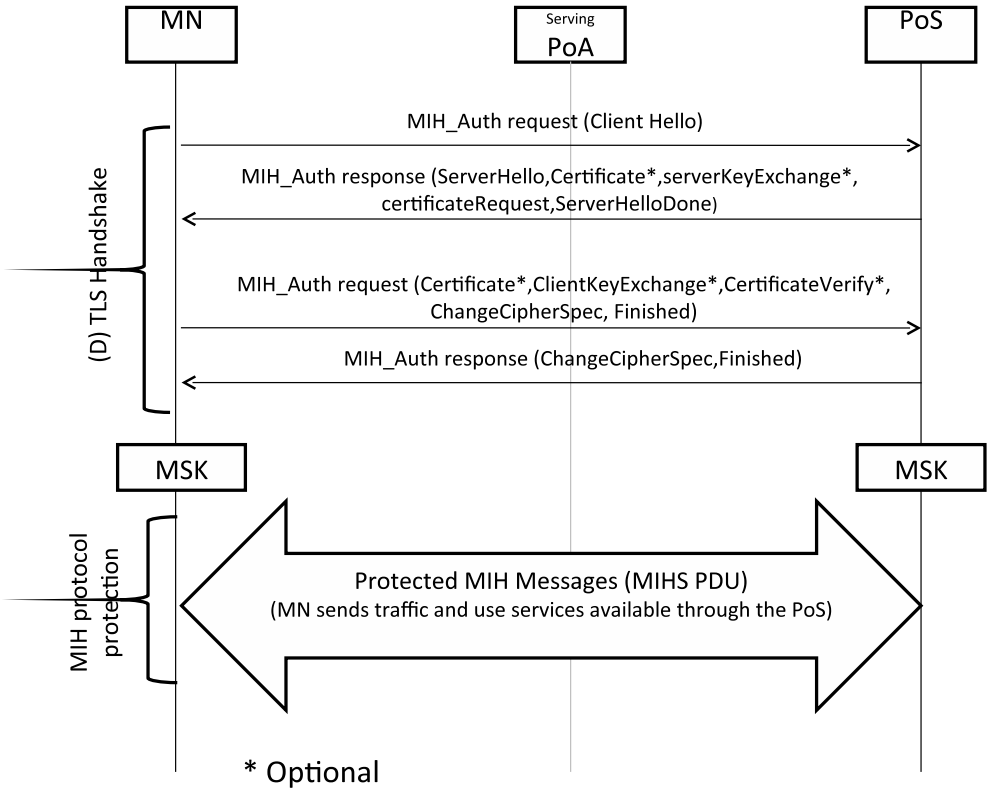
To achieve these goals (authentication and key establishment), IEEE std 802.21a-2012^{TM} introduces two solutions: *TLS-based MIH Message Protection* and *EAP-based MIH Service Access Authentication*. When, for example, PKI access is possible, TLS can be used to protect MIH messages. If MIH services require an authentication through an AAA infrastructure, the *Extensible Authentication Protocol* (EAP) [4] or the *EAP Re-authentication Protocol* (ERP) [5] are used for access authentication and key establishment.

The MN can discover the available options by the exchange of $MIH\_Capability\_Discover$ messages defined in IEEE std 802.21-2008^{TM}. On the other hand, IEEE std 802.21a-2012^{TM} defines a new capability parameter for announcing security capabilities such as service protection, the available proactive authentication mechanisms or ciphersuite.

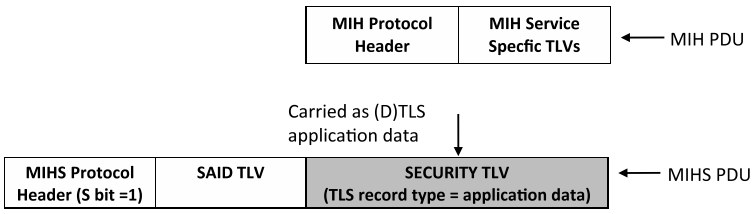
A. TLS-based MIH Message Protection

Let us assume that MN implements (as different wireless devices already do) *Transport Layer Security* (TLS) [6] or *Datagram Transport Layer Security* (DTLS)[1] [7], and decides to establish a protected transport-layer session for securing MIH messages with the PoS. The Standard uses MIH messages to carry (D)TLS handshake and the resulting protected

[1]From now on we use (D)TLS to denote TLS or DTLS.



(a) Establishing MIH SA using (D)TLS



(b) MIH PDU protected by (D)TLS

Fig. 2. MIH Protection using (D)TLS

record datagrams for establishing the security association between MN and PoS. One can think of an alternative approach to this is to assign a port for MIH messages similar to what has been done for *Hypertext Transfer Protocol Secure* (HTTPS) (port 443). However, this works only when MIH messages are carried over IP. In order to make use of TLS even when MIH messages are transported directly over link-layer, it is required that MIH messages transport TLS messages.

So when the MN wants to authenticate the PoS (or vice-versa) with (D)TLS, the former acts as TLS client and the latter as TLS server (Figure 2(a)). During a (D)TLS handshake, the mutual authentication is executed through either a pre-shared key or a public key certified by a trusted third party such as a certificate authority. After the handshake, a (D)TLS session is established. This means the TLS master key and the keys derived from the master key, all of the TLS parameters, and TLS ciphersuite negotiated in the TLS handshake form an MIH *Security Association* (SA). A separate TLV called *Security Association Identifier* (SAID) TLV is defined to carry the MIH SA identifier. After establishing the (D)TLS-based MIH SA, the MN and the PoS protect MIH *Protocol Data Unit* (PDU) as application data (Figure 2(b)). Then the (D)TLS record is transported by a new MIH message in the Security TLV. The S-bit is set in the new MIH message to indicate that an MIH SA exists and the service specific TLVs are protected. The (D)TLS-generated MIH SA can be

terminated through (D)TLS session termination using a new MIH message (MIH_Auth) defined in IEEE std 802.21a-2012^{TM}.

B. EAP-based MIH Service Access Authentication

To better understand how MN and PoS can perform MIH service authentication using EAP-based approach, we provide a brief overview of EAP [4] and ERP [5].

1) EAP and ERP: EAP is a protocol, executed between an *EAP peer* and an *EAP authenticator*, which allows different authentication mechanisms (called *EAP methods*) to conduct an authentication. Several EAP methods are specified in IETF, for example, based on public key, such as EAP-TLS, or symmetric key, such as EAP-GPSK. Most of them support an authenticated key establishment. That is, upon a successful EAP authentication, a key called *Master Session Key* (MSK) is exported from the EAP method to further derive session keys to protect a specific link [8]. The IETF has also developed ERP for fast authentication by using the keys established in a previous EAP execution. Thus, ERP is a symmetric-key based authentication protocol. It exports a *re-authentication Master Session Key* (rMSK) with the same purpose of the MSK. When EAP is used for remote access authentication, a backend AAA server that integrates a EAP/ERP server, is introduced to execute the actual authentication. In this case, an authenticator simply forwards the authentication messages back and forth between the peer and the server. An AAA protocol, such as RADIUS or Diameter, is typically used to transport EAP/ERP messages between the authenticator and the AAA server. On the other hand, the transport of EAP/ERP messages between the peer and the authenticator happens via lower layer transport, known as *EAP lower-layer*.

This model maps to MIH service authentication as follows: MN acts as an EAP peer to authenticate against the PoS that acts as EAP authenticator. PoS can contact a backend EAP server located in the MN's home AAA server for MN's credential verification. MIH protocol is used to transport EAP (or ERP) between the MN and the PoS and, therefore, it is considered as an EAP lower-layer.

2) Basic Operation: Let us assume now that a MN wants to access a service provided by a PoS but the MN discovers that the service requires authentication and authorization based on ERP/EAP. Figure 3 shows an example of authentication based on the EAP-TLS method commonly used in today's deployments. As observed, the MN starts the authentication with a newly defined MIH_Auth message (Step 1). The authentication continues with several exchanges between the MN and the PoS in the **MIH Service Authentication Phase**. Basically the MN and PoS transport ERP/EAP packets through the MIH_Auth message (Steps 2, 3 and 4).

Once EAP/ERP authentication is finished, the MN and the PoS share key material (MSK or rMSK). This key material is used by both entities to protect the different services that MN can request in the **Service Access Phase** (Step 5). In particular, from the MSK/rMSK, a key derivation key *K* is derived. The key *K* is used to further derive a *Media Independent Session Key* (MISK), which is segmented into three keys: the *Media Independent Authentication Key* (MIAK) to provide authentication and key confirmation to the MIH Service Access Authentication Phase (i.e., it allows confirming that MN and PoS participated in the authentication process and, therefore, they have the same keying material); the *Media Independent Encryption Key* (MIEK) and the *Media Independent Integrity Key* (MIIK) to provide confidentiality and integrity to the MIH messages during *MIH Service Access Phase*, respectively.

Finally, if the MN does not want to continue to use the PoS' services or PoS decides to not allow any further access (e.g., session lifetime has expired), they may join in the **Termination phase** (Step 6).

The advantage of using EAP/ERP for PoS service access authentication is that it allows the MN to authenticate and access the services of any PoS connected with the MN's home AAA server. Therefore this approach is preferable when MN is already registered with a backend AAA infrastructure, which is a typical deployment model in today's operator's networks.

IV. Proactive Authentication

Apart from protecting MIH service access, IEEE std 802.21a-2012^{TM} extends the MIH framework to provide a set of new services which reduce the network access authentication latency which, in turn, reduces the overall handover delay. These services are encompassed in the notion of *proactive authentication*. In general, this term refers to an authentication process that allows the MN to prepare a priori the handover security and network access control parameters (e.g., cryptographic keys, session lifetime, and so on) with a particular tPoA to gain faster access when the handover occurs.

IEEE std 802.21a-2012^{TM} defines two options to provide proactive authentication: *Unbundled Media Access Proactive Authentication* and *Bundled Media Access Authentication with the EAP-based MIH Service Authentication*. The former can be used by the MN without a media-independent authentication. The rationale here is the PoS will rely on the fact the MN will have to authenticate anyway with a tPoA to access network service. However, the latter requires the MN to authenticate by using EAP before PoS provides the services.

A MN joining a network can discover if a particular option is available by exchanging $MIH\_Capability\_Discover$ messages with the PoS, which contain a new parameter defined in IEEE std 802.21a-2012^{TM} named $SupportedSecurityCapList$. This parameter contains the supported proactive authentication mechanisms.

A. Unbundled Media Access Proactive Authentication

If the MN decides to use this option (e.g., it does not have any shared credential with the PoS), it sends link-layer authentication frames through a *serving PoS* (sPoS) to the tPoA that is under the control of the sPoS. These media-specific authentication link-layer frames are first tunneled by using unprotected MIH messages (so MIH SA is not required) between the MN and the sPoS. A new message MIH_LL_Auth is used for this purpose. The communication between the sPoS and the tPoA is outside the scope of IEEE

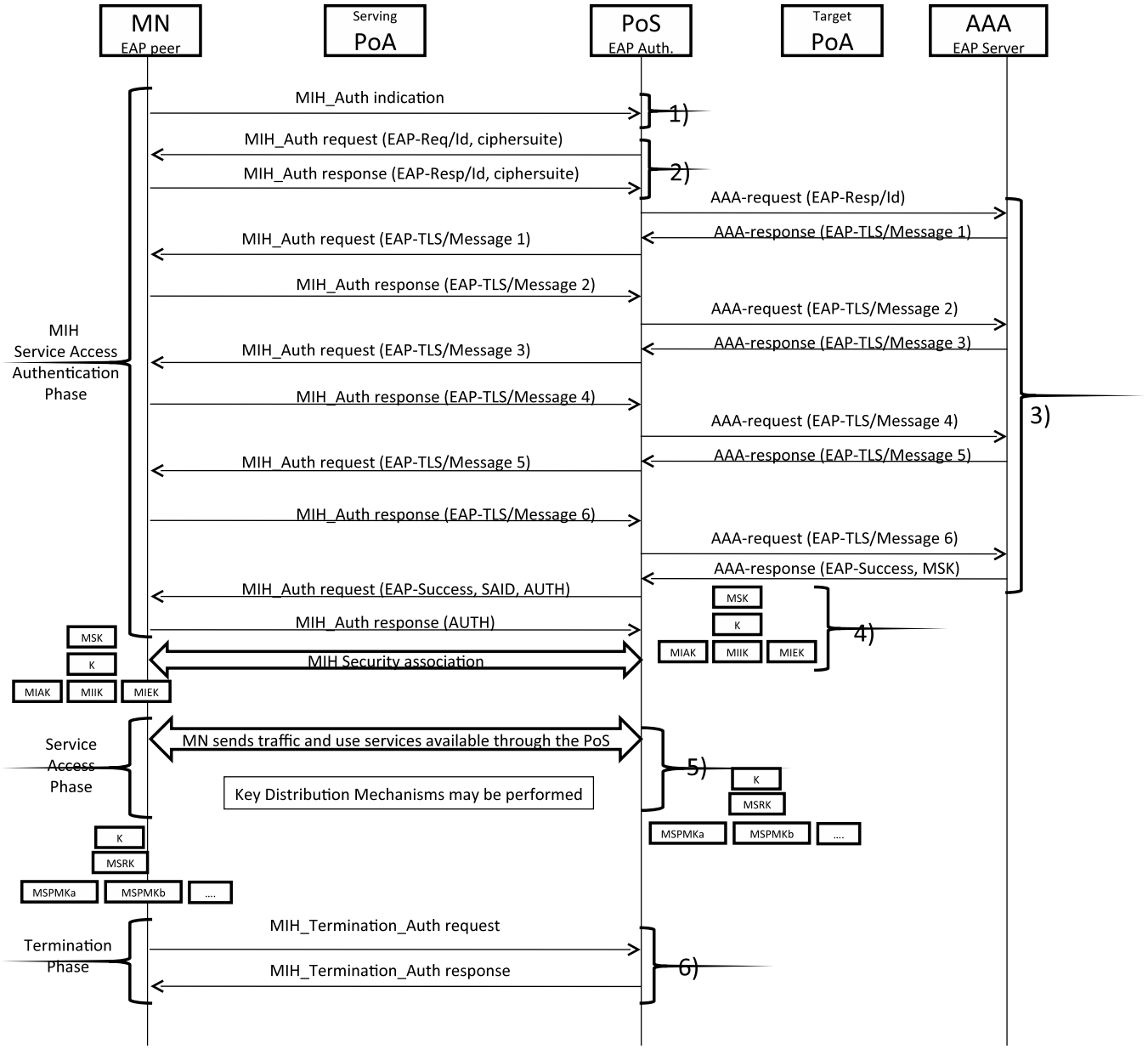


Fig. 3. General EAP-based MIH authentication

802.21a, though a protocol such as *Layer 2 Transport Protocol* [9] may be used.

Figure 4(a) shows that the MN sends media-specific authentication frames to the sPoS by using MIH_LL_Auth messages as transport. Upon reception, the sPoS decapsulates the frames and forwards them to the tPoA. The specific PoA's link-layer identifier (i.e., MAC address) is contained in the MIH_LL_Auth messages.

When the tPoA receives a link-layer authentication frame, it contacts the MN's home AAA server for authentication and authorization. Once tPoA receives an answer, it returns a link-layer frame which subsequently routes to the MN via the sPoS. This process occurs until media-specific authentication is finished. This is equivalent to a normal media-specific authentication. In fact, from the tPoA perspective, it is as if the MN is connecting using a media-specific radio access technology.

At this point the MN and the tPoA have established the shared keying material (MSK). When the MN decides to handover to the tPoA, it can set up data traffic protection with tPoA through performing a security association protocol (e.g., the 4-way handshake specified in IEEE std 802.11-2011^{TM}) using the keying material generated during the proactive authentication.

It is worth noting that certain standards (i.e., IEEE std 802.11-2011^{TM}) provide proactive authentication mechanism, but they are only able to operate within that specific media. The benefit of IEEE std 802.21a-2012^{TM} media-independent transport is that it allows a MN to perform the proactive authentication with the tPoA, even when it belongs to a different access technology or the tPoA is placed on a different network segment.

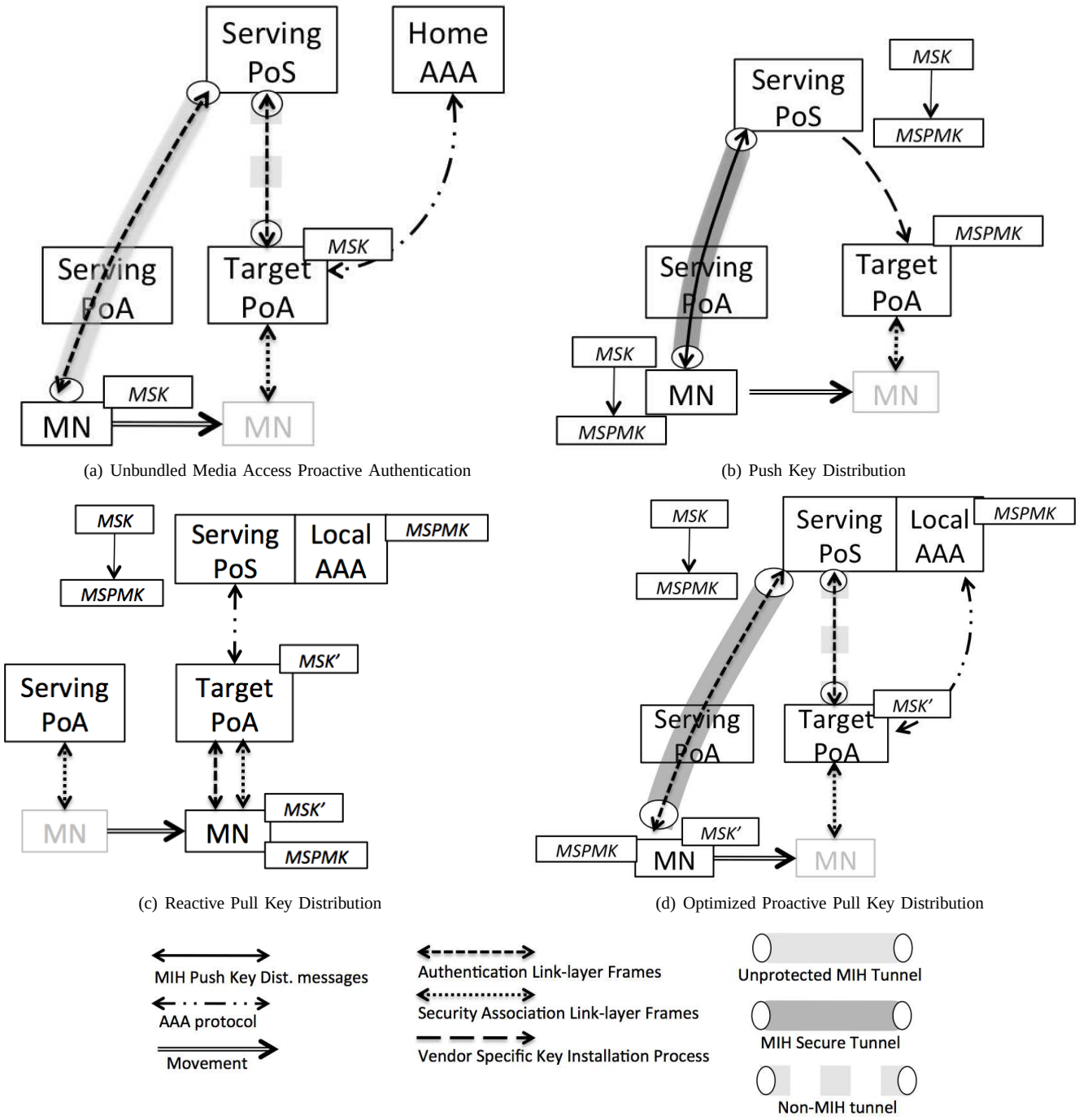


Fig. 4. Proactive Authentication and Key Distribution Mechanisms

B. Bundled Media Access Authentication

In some deployment scenarios, operators may not like to provide the MIH service to the MN without being authenticated with its PoS. In order to support this scenario, a *Bundled Media Access Authentication* option couples the EAP-based MIH Service Authentication described in section III-B with the provision of three key distribution services, which aim to reduce the latency of media specific network access authentication: *Push Key Distribution*, *Reactive Pull Key Distribution* and *Optimized Proactive Pull Key Distribution*. The reason to have several choices is to provide flexible deployment to network operators. The MN can know and select the available key distribution services thanks to $MIH\_Capability\_Discover$ messages with the new parameter $SupportedSecurityCapList$.

Now, let us suppose that a MN wants to use some of these services to reduce the latency to access several tPoAs which are under the control of a *serving* PoS. Then, the MN first runs an EAP-based MIH Service Authentication with the sPoS as described in section III-B. As we know, this authentication provides keying material to protect MIH

services. Nevertheless, IEEE std 802.21a-2012^{TM} has also defined a way to provide an additional set of keys which reduce the latency of media specific access authentication during handover to a tPoA. As depicted in Figure 3 (step 5), the key hierarchy is extended with a new branch where a *Media-Specific Root Key* (MSRK) is derived from the intermediate key *K*. This MSRK is used to derive new session keys, called *Media-Specific Pairwise Master Key* (MSPMK), which are specific to the MN and the tPoA.

Once all the key material is derived, the MN starts one of the available key distribution services with the sPoS so that the MN and the tPoA can re-establish secure access much faster than a typical full authentication.

1) Push Key Distribution: In this model (see Figure 4(b)), the MN requests the sPoS to send (*push*) a key to the tPoA. New MIH_Push_Key messages are used by MN and PoS for this purpose. These MIH messages are protected by the security association established during *MIH Service Access Authentication Phase*. Then, the MN and sPoS derive a specific MSPMK for the tPoA from the MSRK. To complete the process, the sPoS pushes the MSPMK to the tPoA and informs the MN about the result of the installation.

Once the MSPMK has been installed, the MN and the tPoA share the same key and the handover can be initiated. When handover occurs, the MN and tPoA can start a media-specific secure association protocol to protect data traffic without involving any backend element (e.g., authentication server) in the network.

2) Reactive Pull Key Distribution: This mechanism (see Figure 4(c)) enables a procedure to perform a fast media-specific authentication which uses symmetric keys (e.g., ERP). It enables the sPoS to become a local AAA server for the tPoA.

Before the handover, the MN and sPoS derive a new MSPMK for the tPoA, which is kept on hold by the MN and the sPoS. After the MN moves, it starts a regular media-specific authentication with the tPoA. Then, the tPoA contacts the sPoS to complete the authentication instead of contacting the MN's home AAA server. The assumption here is that the sPoS will be topologically nearer than the home AAA server, and hence authentication signalling will not have to traverse all the way to the home AAA server. Thus, the overall latency is reduced.

However, this approach requires the sPoS to implement some AAA server functionality and the MN to have a specific *Network Access Identifier* (NAI) (e.g., $mn@localrealm$). MN's NAI realm is used for the tPoA to forward the authentication request to the sPoS. The correct NAI is provided by the sPoS to the MN during the media-independent authentication.

As a consequence of the media-specific authentication, the sPoS acting as AAA server will send a new MSK (MSK$'$) to the tPoA. This MSK$'$ will be used to establish the SA between the MN and the tPoA.

3) Optimized Proactive Pull Key Distribution: This mechanism (see Figure 4(d)) has certain similarities with the *Unbundled Media Access Proactive Authentication*. Indeed, the MN transports link-layer authentication frames to the tPoA over a MIH-based tunnel between the MN and sPoS; and between the sPoS and the tPoA by means of another type of tunnel. Also, similarly to *Reactive Pull Key Distribution*, the MN and the sPoS derive a MSPMK for the tPoA to perform the media-specific authentication. In this authentication, the sPoS acts as an AAA server and the tPoA contacts the sPoS instead of contacting MN's home AAA server using MN's NAI realm and thereby providing a faster authentication. After successful proactive media-specific authentication, a MSK$'$ is pulled by the tPoA.

However, unlike the *Unbundled Media Access Proactive Authentication*, the link-layer authentication frames are securely transported over protected MIH messages, which implements the MIH-based tunnel. The MIH SA established during the *MIH Service Authentication Phase* performs this protection.

C. Performance Considerations

While IEEE std 802.21a-2012^{TM} discusses several options to reduce the handover latency, it does not provide any guidelines on the use of a particular mechanism for a given deployment scenario. Thus, we discuss some general guidance with respect to the total handover time budget.

Total handover time can be measured by using two components: *handover preparation time* and *handover execution time*. Handover preparation time is typically defined as the time spent before physical connection to the target network is made and handover execution is the time needed to complete the different processes (i.e., link establishment, security association protocol, mobility protocol related signaling) required after the handover. The former does not affect on-going communications since, during this time, it is assumed that the MN is connected to the current network and can send data. However, during the latter, the MN cannot send data. As a result, on-going communications are disrupted.

Thus, it is important to reduce the handover execution time, where the choice of key distribution mechanism is important. Handover execution time for *Unbundled Media Access Proactive Authentication*, *Push* and *Optimized Proactive Pull Key Distribution* are identical: in each case the MN needs to establish a link, to perform a media-specific SA and run the mobility protocol when it attaches to the tPoA. However, *Push Key Distribution* can reduce the handover preparation time more significantly since it only involves a single exchange (MIH_Push_Key request/response).

In *Reactive Pull Key Distribution*, the handover execution time is longer since it also involves a complete authentication with the tPoA after the handover. However, it provides a better deployment model since it does not require any modifications to existing PoAs.

On the other hand, *Unbundled Media Access Proactive Authentication* and *Optimized Proactive Pull Key Distribution* involve a full media-specific authentication that affects the handover preparation time. This may not be an issue for the performance of on-going communications if the process can be started and completed during the handover preparation time. On the other hand, this can be an issue if the MN is moving fast and the handover preparation cannot be complete before it switches to the tPoA.

Mechanism	Pros	Cons	Security	Total Handover Time	
				Handover Prep. Time	Handover Exec.time
Push Key Distribution	Low handoff execution latency. Lowest handoff preparation latency.	It requires an interface to install a key on tPoA from PoS (not standardized yet).	Uses the MIH SA to securely request the key distribution	$T_{MIH^*_{auth}} + T_{MIH_{push}}$	T_{link} + T_{ms-sa} + T_{mob}
Reactive Pull Key Distribution	It does not need any change to the existing wireless standards. Easier deployment	The PoS acts as both the AAA server and the AAA client. Higher handoff execution latency (reactive nature).	Key material is installed in the PoS after a MIH EAP authentication. It performs a media-specific authentication to bring a key to the PoA.	$T_{MIH^*_{auth}}$	$T_{ms-fastauth}$ + T_{link} + T_{ms-sa} + T_{mob}
Optimized Proactive Pull Key Distribution	Low handoff execution latency. Moderate handoff preparation latency: although it involves a full media-specific authentication, it is performed with a near PoS.	It requires the tPoA to accept wireless link-layer frames over a wired link. Thus a network protocol between PoS and tPoA is needed. The PoS must act as an AAA server.	It uses MIH SA to transport the media-specific link-layer authentication frames.	$T_{MIH^*_{auth}} + T_{ms-fastauth}$	T_{link} + T_{ms-sa} + T_{mob}
Unbundled Media Access Proactive Authentication	Low handoff execution latency.	Higher latency at handoff preparation since it always involves a full media-specific authentication with MN's home domain. It requires the tPoA to accept wireless link-layer frames over a wired link. A network protocol between PoS and tPoA is needed.	No MIH SA establishment. It relays in the media-specific authentication with the PoA to trust the MN	$T_{ms-auth}$	T_{link} + T_{ms-sa} + T_{mob}

$T_{MIH^*_{auth}}$: MIH authentication time (*only executed before establishing the MIH SA. Once MIH SA is set this time is not added up)
$T_{MIH_{push}}$: Time of the exchange for requesting Push Key Distribution
$T_{ms-auth}$: Time for performing a media-specific (ms) authentication between the MN and PoA
$T_{ms-fastauth}$: Time for performing a media-specific (ms) fast authentication between the MN and PoA, based on an symmetric key-based protocol
T_{link} : Time for establishing a link-layer association between the MN and the PoA
T_{ms-sa} : Time for performing a security association protocol between the MN and the PoA
T_{mob} : Time required for the MN to perform the mobility protocol

TABLE I
KEY DISTRIBUTION MECHANISM SUMMARY

Table I shows a summary of the pros and cons, security aspects and total handover time[2] of each proactive authentication mechanism. Regarding the latter, a reasonable assumption is that $T_{MIH_{push}} <= T_{ms-fastauth} << T_{ms-auth}$. The reason is that $T_{MIH_{push}}$ represents the time of a roundtrip (two messages) between the MN and PoS for key distribution. In the case of a media-specific fast authentication process ($T_{ms-fastauth}$) we can say that, in the best case, a similar number of roundtrips are required if we use ERP as fast authentication solution. It is worth noting that the media independent authentication time ($T_{MIH^*_{auth}}$) is executed only once with the sPoS. After that, the MN can use the PoS security services without incurring in the $T_{MIH^*_{auth}}$ delay.

V. CHALLENGES AND ON-GOING WORK

When the MN is not allowed to directly communicate with any network element in the target network before the handover, the solution defined in IEEE std 802.21a-2012^{TM} is difficult to be used in its current form. This is because the standard assumes that the MN and the PoS in the target network can communicate via the serving network (where the MN is currently attached). In order to deal with this scenario, a further extension to the standard is needed so that the PoS in the serving network can serve as a relay and forward proactive authentication messages to the PoS in the target network on behalf of the MN.

[2]The total handover time is not exhaustive, while it provides a summary to understand the overall differences between the key distribution mechanisms. More details are available in [10].

Another challenge is to carry not only link-layer authentication frames but also other types of link-layer frames so that higher-layer configuration process of the MN can be proactively carried out. This may require a more generalized approach in which IEEE std 802.21a-2012^{TM} can be considered as a subset of the required building blocks for realizing the generalized proactive operation. These challenges are currently being addressed in IEEE P802.21c, a new amendment project under IEEE 802.21 WG.

VI. CONCLUSIONS

We have provided a comprehensive survey of the IEEE std 802.21a-2012^{TM}, which defines security extensions for *Media Independent Handover* (MIH) Services of IEEE std 802.21-2008^{TM}. We have discussed two main goals defined in IEEE std 802.21a-2012^{TM}: to protect MIH messages to secure signaling in IEEE std 802.21-2008^{TM} services; and to enable mechanisms to reduce handover latency due to security signaling related to network access. For the first goal, two methods have been introduced: (D)TLS based protection, when a PKI is involved; and EAP based authentication and key establishment when AAA infrastructures are deployed. For the second goal, we have analyzed in detail the three key distribution mechanisms defined in the Standard, along with the performance implication to deployment scenarios.

The mechanisms included in this standard are also being discussed in other Task Groups within IEEE 802.21, such as IEEE 802.21c (*Single Radio Handover*) and IEEE 802.21d (*Group Management Solutions*). Thus, it is expected that the

challenges described here will be further discussed and incorporated appropriately in the future versions of the Standard.

ACKNOWLEDGMENT

This work has been partially supported by the Ministry of Science and Innovation, through the Walkie-Talkie project (TIN2011-27543-C03), and partially by the European Seventh Framework Program, through the ITSSv6 Project (contract 270519), and the Seneca Foundation, by means of the GERM program (04552/GERM/06). We finally thank Antonio F. Gomez-Skarmeta for supporting this work and the anonymous reviewers for their valuable comments and suggestions, which have significantly improved the quality of this manuscript.

REFERENCES

[1] *IEEE Standard for Local and Metropolitan Area Networks - Part 21: Media Independent Handover*. *IEEE*, January 2009.
[2] *IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services - Amendment for Security Extensions to Media Independent Handover Services and Protocol*. *IEEE*, May 2012.
[3] Kenichi Taniuchi, Yoshihiro Ohba, V. Fajardo, S. Das, M. Tauil, Yuu-Heng Cheng, A. Dutta, D. Baker, M. Yajnik, and D. Famolari. *"IEEE 802.21: Media independent handover: Features, applicability, and realization"*. In *IEEE Communications Magazine*, pages 112–120, 2009.
[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz (2004). *Extensible Authentication Protocol (EAP)*. RFC3748, June 2004.
[5] V. Narayanan and L. Dondeti. *EAP Extensions for EAP Re-authentication Protocol (ERP)*. RFC5296, August 2008.
[6] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC5246, August 2008.
[7] E. Rescorla and N. Modadugu. *Datagram Transport Layer Security*. RFC4347, April 2006.
[8] B. Aboba, D. Simon, and P. Eronen (2008). *Extensible Authentication Protocol Key Management Framework*. RFC 5247, Aug. 2008.
[9] C. Perkins. *Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*. RFC4719, November 2006.
[10] Fernando Bernal-Hidalgo, Rafael Marin-Lopez, and Antonio F. Gomez-Skarmeta. *"Key Distribution Mechanisms for IEEE 802.21-Assisted Wireless Heterogeneous Networks"*. In *MONAMI'10*, pages 123–134, 2010.

Rafa Marin-Lopez is an assistant lecturer in the Department Information and Communications Engineering at the University of Murcia (Spain). He received B.E., M.E. and Ph.D. degrees in Computer Sciences from the University of Murcia in 1998, 2000 and 2008, respectively. He has collaborated actively in the IEEE 802.21a Task Group and is co-author of IEEE std 802.21a-2012^{TM}. His main research interests include network access authentication, key distribution and security in mobile networks.

Fernando Bernal-Hidalgo is working as researcher and developer in the Department Information and Communications Engineering, University of Murcia (Spain). He has participated in different European Projects such as IST-ENABLE, SWIFT and ITSSv6. He is also co-author of IEEE std 802.21a-2012^{TM}. His main research interests include authentication and authorization in mobile networks.

Subir Das is a Director and Senior Scientist in mobile networking department in Applied Communication Sciences, at New Jersey. His current research interests include mobile networking, network security and mobility, AMI networks, IP Multimedia Subsystem and ad hoc networks. He is very active in several standards and holding leadership positions in IEEE 802. He is a recipient of IEEE Region 1 award and a member of IEEE communication Society.

Lily (Lidong) Chen is a mathematician in Computer Security Division of National Institute of Standards and Technology, USA. She received Ph.D. degree in Applied Mathematics from Aarhus University, Denmark. Her main research interests include cryptography protocols and applications in communication security. She has served as the technical editor for IEEE std 802.21a-2012^{TM}.

Yoshihiro Ohba is a Chief Research Scientist in Toshiba Corporate R&D Center. He received B.E., M.E. and Ph.D. degrees in Information and Computer Sciences from Osaka University in 1989, 1991 and 1994, respectively. He is an active member in IEEE 802 and IETF for standardizing security and mobility protocols. He is Chair of IEEE 802.21a Task Group. He is a main contributor to RFC 5191 (PANA - Protocol for carrying Authentication for Network Access). He received IEEE Region 1 Technology Innovation Award 2008.