Energy Requirements of Secure Vertical Handover Operations in the 802.21a Framework *

Xenofon Foukas†, Dimitrios Loukatos†, Kimon Kontovasilis†, Hugo Marques‡
†Institute of Informatics & Telecommunications, NCSR ”Demokritos”, Greece
{xfoukas, dlouka, kkont}@iit.demokritos.gr
‡ 4TELL Group, Instituto de Telecomunicações, Portugal
hugo.marques@av.it.pt

***Abstract*—IEEE 802.21 is a widely accepted standard providing a media-independent framework and services for enabling seamless handovers among heterogeneous wireless environments. The IEEE 802.21a standard complemented the original specification in an important direction, namely the provision of security mechanisms for handover-related signaling messages and services. However, although the new standard gives a detailed description of the incorporated security mechanisms and of the relevant changes to the structure of the signaling messages, it does not discuss the pros and cons of each security method, with respect to their energy efficiency. This work attempts to fill this gap, by providing simple yet descriptive analytical expressions for calculating the additional energy expended in mobile devices under handover due to the 802.21a security enhancements. These expressions are validated through measurements on a prototype heterogeneous network testbed. The results provide useful hints when choosing the appropriate protection method in devices with tight energy constraints.**

I. Introduction

Current wireless networking environments are characterized by the availability of multiple coexisting wireless access technologies, such as IEEE 802.11, IEEE 802.16, UMTS and LTE, among others. The IEEE 802.21 standard [1] enables seamless vertical handover (VHO) operations between these technologies by means of a Media Independent Handover (MIH) framework, which provides an abstraction layer that hides the low level details (access technology specifics) and expresses the higher level VHO related operations (commands, notifications for network events, etc.) in uniform terms.

One shortcoming of the original IEEE 802.21 standard was the complete lack of protection mechanisms for handover-related signaling messages and services. The problem lies in the fact that the entities participating in MIH procedures do not have any means of authentication and authorization and therefore cannot be trusted, while all MIH related messages are transmitted completely unprotected (at the 802.21 protocol level) and could be monitored or modified by a malicious entity. This lack of protection can raise a number of security threats, like data tampering and traffic analysis attacks [2], [3], compromising the integrity and privacy of mobile devices.

To overcome this, IEEE developed the 802.21a standard [4] to define security extensions for the original MIH protocol. The main new elements are: (i) the introduction of cryptographic algorithms in the protocol for the protection of VHO related messages; (ii) the development of a mechanism for (mutual) authentication between a Mobile Node (MN) and the entity providing the MIH services; and (iii) the inclusion of a proactive authentication mechanism between the MN and its Point of Attachment (PoA) (e.g. a base station) to the network after the VHO has been completed, which aims at reducing the latency of the whole VHO process.

In the present world of battery-limited devices, improving the energy efficiency of costly operations is a very important factor. While the capability for secure VHOs undeniably leads to the enhancement of the overall service experience, it comes at a high cost in terms of energy consumption. In this paper we investigate, both analytically and through measurements, the additional energy in mobile devices due to the VHO related security operations, according to the 802.21a framework. Knowing this overhead can aid in making smart decisions for VHO protection, effectively increasing the energy-efficiency of mobile devices.

There have been several prior works studying the energy-efficiency of mobile devices from various relevant viewpoints. One line of research has looked at the development of mechanisms for reducing the energy consumption at devices with multi-radio capabilities, through a better exploitation of the alternative radio interfaces [5], [6], [7]. In relation to the cost of security operations, [8] and [9] study the energy consumption characteristics of various security algorithms like AES and protocols like SSL through measurements on a PDA device. Similarly, [10] and [11] address the energy consumption of various security algorithms in wireless sensor motes. From a perspective similar to the one adopted by the present paper, [12] investigates the energy requirements associated with the execution of VHOs in 802.21, through a prototype heterogeneous network testbed that employs ACPI-assisted energy measurements.

Despite the existence of the prior works just mentioned, the additional energy requirements for applying the 802.21a security mechanisms to MIH messages has not been investigated yet, to the best of the author’s knowledge. This work attempts to fill this gap, having two main goals. The first is to provide an analysis of the additional signaling overhead due to the protection mechanisms defined in 802.21a. The analysis leads to simple expressions for the calculation of the associated energy expenditure as a function of relevant parameters. The second goal is to evaluate the validity of these expressions, through measurements taken on actual mobile devices and to provide comparative results that are of help in choosing the proper protection method in 802.21a enabled devices with tight energy constraints.

The remainder of this paper is structured as follows: Necessary background on IEEE 802.21 and its security extensions is given in Section II, while Section III takes up on the analysis of the security-related energy overhead in 802.21a VHO operations. Section IV presents the measurement methodology

* Work supported by the European FP7 project GREENET (FP7-PEOPLE-2010-ITN-264759).

and discusses experimental results. Finally, conclusions are drawn in Section V.

II. Overview of 802.21 and its security extensions

A. Message structure and timing in 802.21

The IEEE 802.21 defines [1] a Media Independent Handover (MIH) framework for performing handovers between heterogeneous networks. At the core of the 802.21 framework lies the Media Independent Handover Function (MIHF), responsible for providing handover services to the upper layer (MIH User) through a media independent interface. The MIHF consists of three types of services, namely: Media Indepenedent Event Services (MIES), which detect the change in link behaviors and generate the appropriate events for both local and remote MIHFs; Media Indepenedent Command Services (MICS), which control the link state; and Media Independent Information Services(MIIS), which provide mechanisms for an MIH entity to discover and obtain information about candidate networks (CNs), .i.e., networks collocated with the serving network that are potential handover targets.

The communication between MIH entities occurs by exchanging MIH protocol messages. As illustrated in Fig. 1, a typical MIH message contains a protocol header and a payload composed of several information elements, represented in Type-Length-Value (TLV) format. The MIH protocol header carries essential information used for parsing and analyzing the frame, while the payload carries identifier TLVs for the source and the destination MIHF of the message and a number of MIH service specific TLVs carrying protocol related information. It should be noted that the length of the source and destination identifiers is not specified in the standard.

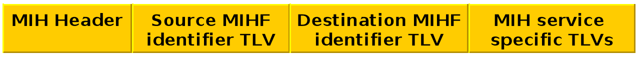
MIH Header
Source MIHF identifier TLV
Destination MIHF identifier TLV
MIH service specific TLVs

Fig. 1: Structure of a typical MIH message

When a VHO is triggered in an 802.21 enabled environment, a number of MIH message exchanges occur between the MN and an entity located in its serving network, the, so called, Point of Service (PoS) within the MN's serving network. The PoS is an entity responsible for providing MIH related services to mobile devices. A VHO can be initiated either by the MN or by the serving network, depending on the nature of the handover trigger. For example, an MN might initiate a VHO in case the signal strength of its link to the serving network drops below some acceptable threshold, while a network initiated VHO might be caused by a highly congested network attempting to offload some of the connected MNs to other collocated wireless networks.

The messages sequence in a typical MN initiated VHO procedure is illustrated in Fig. 2. Initially, the MN makes an information request to a MIIS in order to gather static information about the characteristics and services of the available CNs in range. Using the reply, the MN performs a scan to determine and retain those of the CNs in the reply that actually provide it a radio link of sufficient quality. After this verification, the MN performs a query to its serving PoS, requesting a resource availability check at the (retained) CNs. The PoS is responsible to query each of the CNs indicated by the MN for resources and to inform the MN of the outcome, by providing a list of candidate networks that actually have adequate resources for the needs of the MN. Subsequently, the MN selects one among those CNs as the handover target on the basis of a policy and informs the serving PoS, requesting the allocation of the required resources on the target CN. Once the resources are allocated, the MN is informed by the PoS and proceeds into establishing a Layer 2 connection with the PoA of the target network, also performing other related operations, like the authentication of the MN by the target network. When the handover is completed at the higher layers, the MN informs the target PoS, which becomes the new serving PoS and informs the old one of the handover completion, so the latter can release the resources allocated for the MN.

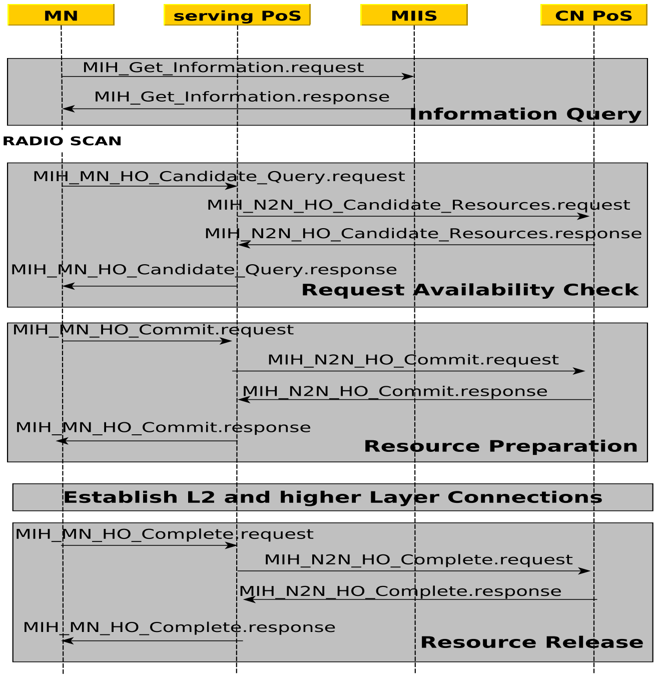
MN
serving PoS
MIIS
CN PoS
MIH_Get_Information.request
MIH_Get_Information.response
Information Query
RADIO SCAN
MIH_MN_HO_Candidate_Query.request
MIH_N2N_HO_Candidate_Resources.request
MIH_N2N_HO_Candidate_Resources.response
MIH_MN_HO_Candidate_Query.response
Request Availability Check
MIH_MN_HO_Commit.request
MIH_N2N_HO_Commit.request
MIH_N2N_HO_Commit.response
MIH_MN_HO_Commit.response
Resource Preparation
Establish L2 and higher Layer Connections
MIH_MN_HO_Complete.request
MIH_N2N_HO_Complete.request
MIH_N2N_HO_Complete.response
MIH_MN_HO_Complete.response
Resource Release

Fig. 2: MN initiated VHO

The network initiated VHO case is very similar to the MN initiated case just described, the main difference being that the PoS is responsible for consulting the MIIS instead of the MN. Still, the information obtained by the PoS through this action is subsequently transmitted to the MN, so the total number of messages exchanged during the VHO remains the same as in the process described. Another point of notice is that large MIH messages could be fragmented, leading to a longer message sequence. However, for most realistic scenarios this is not the case, so the total number of messages during a VHO, from the point of view of the MN, can be considered to be equal to the one illustrated in Fig. 2.

B. Security extensions in IEEE 802.21a

The 802.21a standard defines two protocols that can be used for protecting MIH messages. When Public Key Infrastructure (PKI) access is possible, messages can be protected using a TLS-based protection mechanism [13]. On the other hand, if the authentication of MIH messages is required through an Authentication, Authorization and Accounting (AAA) infrastructure, the Extensible Authentication Protocol (EAP) [14]

TABLE I: 802.21a ciphersuites for EAP-based protection

Ciphersuite	Type of protection	Overhead (Bytes)
AES-CCM	Authenticated Encryption	22
AES-CBC+ HMAC-SHA1-96	Encryption and authentication	44
HMAC-SHA1-96	Authentication & Integrity	12
AES-CMAC	Authentication & Integrity	12

or the EAP Reauthentication Protocol (ERP) [15] can be used for access authentication and key establishment. In both cases, the standard defines the procedures and message exchanges required for establishing a security association (SA) between two entities. At the end of this process, each participating entity ends up having a master session key (MSK), which is used for generating all the keys required for applying the security algorithms over MIH messages. The 802.21a standard supports a wide number of ciphersuites according to the protection protocol employed. Specifically, EAP/ERP can use the ciphersuites listed in Table I, while TLS may employ all ciphersuites defined in its specification [13].

An MIH message protected according to the 802.21a standard has a slightly different structure compared to that of the original MIH protocol, as illustrated in Fig. 3. The length of the MIH header remains unaltered and the only difference in its contents is that two bits reserved for future extensions in 802.21 are now being used to indicate that this message is protected and/or that it is intended for the authentication of the MIHF. Moreover, the entities participating in an MIH message exchange (MN and PoS MIHFs) can be uniquely identified by the SA they have established. Therefore, source and destination identifiers in messages are no longer required and are replaced by an SA Id (SAID) TLV. The final part of an MIH message is composed of the service specific TLVs, which are encapsulated in a Security TLV, after applying the required protection mechanisms. As with the source and destination Ids in the original 802.21 specification, the 802.21a standard does not define a specific length for the SAID.

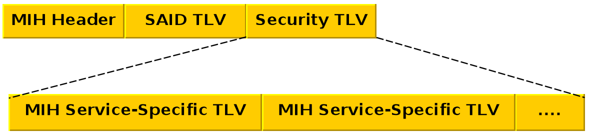

Fig. 3: Structure of a protected MIH message

The security TLV is integrity protected and authenticated. To this end, a Message Integrity Code (MIC) is appended at the end of the security TLV, after the service-specific TLVs. Depending on the level of protection required, the security TLV might also be additionally encrypted. In this case an extra overhead is involved, since various additional information items (e.g., a Serial Number - SN or an Initialization Vector - IV) need to be carried by MIH messages, depending on the ciphersuite employed. The total overhead incurred by each protection method supported by EAP/ERP is described in [4] and listed in the final column of Table I. TLS ciphersuites incur similar overheads, omitted here due to lack of space.

III. 802.21a Energy Overhead in VHOs

We now discuss the energy overhead of the operations introduced in 802.21a. In particular, we focus on the energy overhead associated with the application of protection mechanisms over MIH messages, once a VHO is triggered. The analysis excludes ”one-off” initialization/set up operations. While the energy consumption of such operations (e.g., establishment and exchange of keys, or proactive authentication) can also be significant, it is unavoidable for the device and is the same regardless of the ciphersuite employed. By contrast, the particular MIH message protection method can be chosen among alternatives, so the issue of identifying the method that meets the minimum user requirements and is most energy-efficient justifies further study.

Accordingly, for the remainder of this paper it is assumed that prior to the initiation of a VHO procedure, an MN has been authorized to access the MIH services provided by some MIH entity, after (mutually) authenticating using (D)TLS or EAP/ERP, as defined by 802.21a. This implies that an SA has been established between the MN and a PoS and an MSK has been generated and is being held by the participating entities.

To determine the energy overhead, one must first assess the additional data carried in MIH messages, on the basis of the message structure and other details discussed in Subsection II-B. To this end, the standard [4] provides the following simple expression for the total security overhead, O_{sec}, in an MIH message:

$$\begin{aligned} O_{\text{sec}} = L_{\text{SAID}} - (L_{\text{SID}} + L_{\text{DID}}) + O_{\text{SECTLV}} \\ + O_{\text{TYPE}}(y) + yO_{\text{TLS}} + O_{\text{enc/intg}}, \quad y = 0, 1. \end{aligned} \tag{1}$$

With respect to the parameters involved in (1), L_{SAID}, L_{SID} and L_{DID} are, respectively, the lengths of the SAID TLV and of the source and destination identifiers replaced by the SAID TLV. O_{SECTLV} is the overhead of the security TLV carried in the protected MIH message. It has a size of 3 bytes (1 for TLV type and 2 for TLV length). The parameter y signifies whether an SA is established through TLS ($y = 1$) or EAP/ERP ($y = 0$). The structure of (1) reflects that a TLS SA has an additional overhead O_{TLS}, due to the TLS record. O_{TLS} has a value of 5 bytes (1 for TLS type, 2 for version and 2 for length). $O_{\text{TYPE}}(y)$ is the overhead of the MIH data type contained in the security TLV. The standard defines that this field will have a length of 6 bytes for $y = 0$ (EAP SA) and 3 bytes otherwise. The final parameter is $O_{\text{enc/intg}}$, which is the overhead incurred by the bits used for encryption, integrity protection and authentication. This overhead depends on the ciphersuite employed. When an EAP/ERP ciphersuite is used, the overhead can be found in Table I. For TLS protection, the overhead is determined similarly, according to the TLS protocol specifications [13].

Given the security overhead (1), one can calculate the mean energy spent for applying protection mechanisms in MIH messages during a VHO. We are interested in studying the energy overhead from the point of view of the MN, due to its battery constrained nature. Thus, we concentrate on messages sent or received by the MN. The energy expenditure can be divided into two parts; the energy for exchanging the protected MIH messages and the energy for applying the security operations (encryption, decryption, integrity checks etc.). In relation to the first part, the base cost of transmitting the service specific TLVs will be the same regardless of the protection method employed. Therefore, we focus on computing the additional energy spent for transmitting/receiving the extra protection bits. The mean energy cost, E_{comm}, for the communication part is

$$E_{\text{comm}} = O_{\text{sec}}(N_{\text{Tx}}E_{\text{Tx}} + N_{\text{Rx}}E_{\text{Rx}}). \tag{2}$$

N_{Tx} and N_{Rx} are the number of messages transmitted and received by the MN, respectively, for a given VHO scenario. As discussed in Section II-A, the number of messages during a handover can vary (e.g., due to the fragmentation of a large MIH message sent by the MIIS). However, the message sequence presented in 2 applies for most realistic scenarios, therefore both of N_{Rx} and N_{Rx} would typically be equal to 4. The quantity E_{Tx} (resp. E_{Rx}) is the mean energy spent by the MN for the transmission (resp. reception) of a unit of data. Typical values for these parameters are available through measurement based works, e.g., [6].

Similarly to (2), the mean energy overhead of the MN for the security operations applied to the messages of a VHO scenario is

$$E_{\text{sec}} = L_{\text{MIH}}(N_{\text{Tx}}E_{\text{enc/intg}} + N_{\text{Rx}}E_{\text{dec/intg}}), \tag{3}$$

L_{MIH} is the mean length of the protected part of the MIH message, i.e., the mean length of the service specific TLVs. $E_{\text{enc/intg}}$ is the mean energy for integrity protecting, authenticating and encrypting (when applicable) one unit of data in a transmitted MIH message. Respectively, $E_{\text{dec/intg}}$ applies to incoming messages and is the mean energy for applying the reverse actions on a unit of data. Again, typical values for these energies can be obtained through measurement works, e.g., [8], [9].

IV. Energy Consumption Measurements and discussion

A. Energy measurement methodology

The energy measurements followed the methodological approach in [12], employing mobile devices supporting the Advanced Configuration and Power Interface (ACPI) and observing changes to the ACPI status as a means of measuring energy expenditure. As a preprocessing step, ACPI based measurements are used for determining the mean power consumed when the device is in an idle state. This corresponds to the average consumption for periodic operating system maintenance tasks. Subsequently, the task to be measured (e.g., MIH message exchanges) is repeatedly executed for a sufficiently long period of time and the overall energy spent during this period is observed. Since both the overall energy and the energy spent for maintenance tasks during this period of time are known, it is trivial to compute the mean energy spent for the actual task under study, by dividing the difference of these energies by the number of task execution repetitions.

Application of the methodology just described to the tasks that are of interest in this work was simple and intuitive and proceeded as follows: Initially, various VHO scenarios were executed using the original 802.21 protocol in a prototype testbed (the same as the one employed in [12]). This process produced real MIH messages with typical content. The generated messages were captured and analyzed to determine the mean length, L_{MIH} of their payload. Subsequently, the captured messages were stored in binary files, properly distributed between the MN and the PoS, with request messages stored in the MN and reply messages in the PoS. The VHO scenario was then replayed in an off-line "dummy" manner. Specifically, for each MIH request message sent by the MN, the already stored, corresponding reply message was sent back from the PoS without actually performing 802.21 processing on the request. The energy consumed for executing the whole scenario off-line, as well as the energy for transmitting and receiving one unit of data (E_{Tx}, E_{Rx}) were measured in the MN, using the methodology previously described. The messages were stored in the RAM of the MN before executing the scenario, in order to avoid disk reads/writes that would distort the measurements for the total energy overhead.

In a second phase, the scenarios were replayed with the 802.21a extensions enabled and the corresponding energy consumptions were measured again. This phase involved a transformation of the original MIH messages into the form specified by 802.21a. To this end, each file containing stored messages for a VHO scenario was converted to include the same messages, but stripped from those fields not used in 802.21a (source and destination IDs). Subsequently, for each stripped MIH message loaded in RAM, a SAID TLV was created and appended to the message, while the service specific TLVs were encapsulated in a security TLV, protected by one of the methods defined in 802.21a, as described in Section II-B. Then, the energy consumed for executing the security enabled scenarios off-line, as well as that for applying individual security operations ($E_{\text{enc/intg}}$, $E_{\text{dec/intg}}$), were measured in the MN.

With this two-phase process, the energy overhead for the 802.21a security enhancements was obtained simply by subtracting the energy measured in the first phase from the energy measured in the second phase. It is noted that, as already mentioned, this work focuses on the energy overhead of the protection methods applied over MIH messages, rather than the overhead associated with authentication and key distribution. In alignment with this, an MSK and a SAID were generated and distributed in both the MN and the PoS before proceeding with the measurements.

B. Results

The measurements were taken on an eight-core Lenovo T530 notebook equipped with an Intel Centrino WLAN module, acting as the ACPI-featuring MN. The exchange of MIH messages employed UDP transport over WiFi. OpenSSL 1.0.1.h-1 was employed for the security operations. The ciphersuites that were studied are those listed in Table I for EAP/ERP.

Table II lists the length of the source, destination and SA Ids, as used in the experiments. The values of the parameters (which as already mentioned are not specified in the standard) are typical and coincide with these used in the prototype testbed [12]. The mean length of the service specific TLVs, as determined from the MIH messages actually generated, is also listed in the table. Table III lists the individual security and communication energies per unit of data processed, as determined from the experiments. The (-) symbol signifies operations not supported by the corresponding ciphersuite.

TABLE II: Length of SID, DID and SAID and mean length of the service specific TLVs in bytes

L_{SID}	L_{DID}	L_{SAID}	L_{MIH}
20	20	30	131.5

The total amount of the additional energy consumed per VHO, as obtained through the expressions (2) and (3) and through the experiments is illustrated in Fig. 4. It can be

TABLE III: Energy measurements (J/bit) for security and communications operations when using the UDP protocol

(a) Security operations

Ciphersuite	Enc	Dec	Intg
AES-CCM	4.2e-9	4.18e-9	-
AES-CBC+ HMAC-SHA1-96	3.8e-9	9.08e-10	3.36e-9
HMAC-SHA1-96	-	-	3.36e-9
AES-CMAC	-	-	4.28e-9

(b) Communication

Tx
4.6e-7

Rx
4.19e-7

seen that the theoretically predicted and the experimentally determined values maintain the same trends, over all protection methods considered. Moreover, the difference between analytical expressions and experimental results is seen to be close to 15% almost uniformly over all cases. This difference is small enough, perhaps smaller than the one expected, given the multitude of the various ”noise” operations and implementation-dependent idiosyncrasies present in a real-life testbed (each such factor contributing its small, unanticipated energy expenditure) and the small magnitude of the energies whose measurements were sought. Overall, the results validate the theoretically derived expressions (2) and (3), indicating that they successfully account for all important factors contributing to the additional energy expenditure they address.

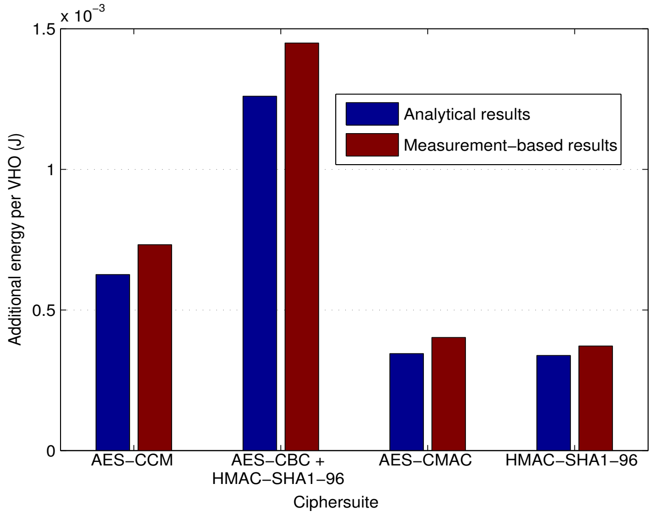

Fig. 4: Additional energy incurred by applying 802.21a protection methods

An important thing to notice is that the energy efficiency is just one of the parameters to be taken into consideration when choosing the proper protection method for MIH messages. An equally important aspect to consider is the protection level that the user requires. For instance, even though HMAC-SHA1-96 is the most energy efficient method out of the four studied in this paper, it would not be considered a good choice for guarding against traffic analysis attacks. AES-CCM would instead be considered a better choice, since it not only offers integrity protection and authentication of messages but also encryption. At the same time this method is more energy efficient than AES-CBC + HMAC-SHA1-96, which offers the same level of protection and, therefore, is considered a more reasonable choice. It is this type of choices that highlight the usefulness of our energy analysis when specific user requirements need to be met. In closing, we note that, although the experiments did not examine TLS, the principles of our methodology are not affected, since the only thing that would change in the case of a TLS-based handover would be the different amount of energy consumed by the TLS ciphersuites as well as the security overhead of (1).

V. Conclusions

This paper presented an analysis of the energy requirements for the protection of VHO related messages using the security extensions defined in 802.21a. Analytical expressions were formulated by taking into consideration the energy expenses of individual security and communication actions and the size overhead incurred in MIH messages due to the structural changes caused by 802.21a. These expressions were validated through actual measurements taken from a prototype heterogeneous network testbed, demonstrating the suitability of various protection methods when specific requirements from both an energy and a security perspective need to be met.

References

[1] “IEEE standard for local and metropolitan area networks - media independent handover services,” *IEEE Std 802.21-2008*, Jan 2009.

[2] I. Saadat, F. Buiati, D. R. Cañas, and L. J. G. Villalba, “Overview of IEEE 802.21 security issues for MIH networks,” in *ICIT 2011: Proceedings of the 5th International Conference on Information Technology*, 2011.

[3] T. Melia, G. Bajko, S. Das, N. Golmie, and J. Zuniga, “IEEE 802.21 mobility services framework design (MSFD),” *IETF draft*, 2009.

[4] “IEEE standard for local and metropolitan area networks: Media independent handover services - amendment for security extensions to media independent handover services and protocol,” *IEEE Std 802.21a-2012 (Amendment to IEEE Std 802.21-2008)*, pp. 1–92, May 2012.

[5] T. Pering, Y. Agarwal, R. Gupta, and R. Want, “Coolspots: reducing the power consumption of wireless mobile devices with multiple radio interfaces,” in *Proceedings of the 4th international conference on Mobile systems, applications and services*. ACM, 2006, pp. 220–232.

[6] N. Balasubramanian, A. Balasubramanian, and A. Venkataramani, “Energy consumption in mobile phones: a measurement study and implications for network applications,” in *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*. ACM, 2009, pp. 280–293.

[7] A. Rahmati and L. Zhong, “Context-for-wireless: context-sensitive energy-efficient wireless data transfer,” in *Proceedings of the 5th international conference on Mobile systems, applications and services*. ACM, 2007, pp. 165–178.

[8] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, “Analyzing the energy consumption of security protocols,” in *Proceedings of the 2003 international symposium on Low power electronics and design*. ACM, 2003, pp. 30–35.

[9] ——, “A study of the energy consumption characteristics of cryptographic algorithms and security protocols,” *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128–143, 2006.

[10] J. Lee, K. Kapitanova, and S. H. Son, “The price of security in wireless sensor networks,” *Computer Networks*, vol. 54, no. 17, pp. 2967–2978, 2010.

[11] J.-P. Kaps and B. Sunar, “Energy comparison of AES and SHA-1 for ubiquitous computing,” in *Emerging directions in embedded and ubiquitous computing*. Springer, 2006, pp. 372–381.

[12] D. A. Wassie, D. Loukatos, L. Sarakis, K. Kontovasilis, and C. Skianis, “On the energy requirements of vertical handover operations: Measurement-based results for the IEEE 802.21 framework,” in *IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2012, pp. 145–149.

[13] T. Dierks, “The transport layer security (TLS) protocol version 1.2,” 2008.

[14] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz *et al.*, “Extensible authentication protocol (EAP),” RFC 3748, June, Tech. Rep., 2004.

[15] V. Narayanan and L. Dondeti, “EAP extensions for EAP re-authentication protocol (ERP),” 2008.