# Lightweight Authentication and Key Management on 802.11 with Elliptic Curve Cryptography

Suneth Namal*, Konstantinos Georgantas† and Andrei Gurtov*
*Centre for Wireless Communications
University of Oulu, Finland
†Helsinki Institute for Information Technology
Helsinki, Finland
Email: [namal, gurtov]@ee.oulu.fi, [konstantinos.georgantas, gurtov]@hiit.fi

***Abstract*—Wireless Local Area Networks (WLANs) have experienced a significant growth during the last decade due to ever emerging and heavy resource demanding applications. Widely used IEEE 802.11 may unexpectedly require long durations in association compared to what Voice over IP (VoIP), Video on Demand (VoD) and other real-time applications can tolerate. In this paper, we implement HIP-WPA; a novel approach of Fast Initial Authentication (FIA) which is a combination of Host Identity Protocol Diet EXchange (HIP-DEX) with some features of Wi-Fi Protected Access (WPA) technology. This approach provides the necessary IP layer elevated security mechanisms in order to face the challenges of fast authentication in WLANs. HIP-DEX introduces a radically new way of authenticating hosts by using Elliptic Curve Cryptography (ECC) only with two message exchanges and therefore improves the authentication delay by 300% compared to WPA2. Thus, this is an effective solution to be used with any type of real-time application for intra-network (Basic Service Set (BSS) transitions) and inter-network (Extended Service Set (ESS) transitions) handovers.**

## I. Introduction

The technology advances during the last decade have contributed the most to the development of portable mobile devices. IEEE 802.11 standard has a major impact on broadly using mobile devices in every aspect of human life. This protocol enables WLAN connectivity and introduces mobility for wireless devices. On the other hand, mobile subscribers prefer VoIP applications due to the reduced cost. However, cellular networks are bandwidth limited; thus, VoIP applications pose strict constrains when they are used over cellular access.

IEEE 802.11 networks are favorable to VoIP applications because of the high data rate they can support. The above statement is not always valid in mobile environments where mobile STAtions (STAs) are moving between the BSSs; especially when they experience a short dwell time within an Access Point's (AP) coverage area. It is also not true when a large number of users closely (in time scale) entering to an ESS for the first time. More specifically, host mobility introduces the following four serious problems [1]:

- **Addressing :** When a host is attached to a new AP, it finds out that it has a topologically invalid address.
- **Location management :** Changing the IP address to solve the latter issue creates additional overhead as the mobile STA must also inform its peer nodes.
- **Session maintenance :** Changing an IP address may also tear down active connections. IP addresses are often used as part of the connection identifiers. Higher layers are sensitive to disconnections.
- **Secure handover :** This also includes reauthentication and often reassociation.

Moreover, network architectures in the name of backward compatibility and incremental upgrades are supported from the beginning with multi-layered design. Thus, wireless networks by themselves are insecure and the media that they use, impose each and every network layer to perform similar authentication and authorization security mechanisms [2], [3]. In pure mobility cases, the above implementation is simply inefficient.

In this paper, we focus on the delay that the current initial authentication process introduces to an AP when a mobile STA is entering to an ESS for the first time as well as the delay in link establishment. Fast authentication is what mobile stations need in order to experience real mobile services. The implementation can help in this direction as it presents a new cryptographic namespace which identifies hosts and therefore allows the network layer to be decoupled from upper layers with improved security and mobility. This means that duality property of IPs' both as host identifiers and locators is removed [4], [5], [6]. Therefore, this implementation can also give solutions to multi-homing, mobility and security.

The rest of this paper is structured as follows: Section II describes the current authentication methods of Robust Security Networks (RSNs). Section III describes the weaknesses and challenges of today's FIA solutions. In section IV, we present our novel approach of HIP-WPA. The implementation methodology is described in the Section V whereas the experimental results are illustrated in Section VI. Finally, in Section VII we discuss the potential barriers in FIA and conclude our research in Section VIII.

## II. FAST INITIAL AUTHENTICATION

FIA is what mobile stations need in order to merge in real mobile services. The cost of it seems really low as it does not include hardware changes but only some modifications of the 802.11 standards which can possibly be integrated to or form a new amendment of the existing standard. FIA aims in three basic amendments of the IEEE 802.11 standard [7]. FIA could possibly improve or satisfy the below listed challenges.

- Support for a large number of simultaneously entering mobile STAs in an ESS.
- Support for small dwell time (due to high velocity and small cell areas) in an Extended Service Area (ESA).
- Secure initial authentication. FIA's scope is only within the authentication and association processes, neither the AP Discovery nor the upper layer link setup such as Dynamic Host Configuration Protocol (DHCP).

During the past years, there were no many activities related to FIA as far as security is concerned. IEEE 802.11 standard defines two types of authentications; i.e. Open System (OSA) and Shared Key. With OSA, a STA can join any network and receive messages that are not encrypted. Wired Equivalent Privacy (WEP) was the first security choice for WLAN users, though it was weak and cracked. In order to enhance the WEP encryption, WPA framework which supports Temporal Key Integrity Protocol (TKIP) with RC4 stream cipher was introduced. Authentication of WPA clients is done with a key which is dynamically generated or shared between the authenticator and the supplicant. IEEE 802.11 amendment introduces the concept of RSNs. RSNs use Counter mode with Cipher block chaining Message authentication code Protocol (CCMP), which makes use of the Advanced Encryption Standard (AES), as far as the encryption method is concerned. This enhancement to WPA is also known as WPA2.

### A. *FIA proposed solutions*

There are already some proposed solutions that could possibly mitigate the challenges in Section II. Most of them rely on the existing authentication mechanisms and try to reduce the number of exchanged packets by modifying the 802.1x/EAP authentication process. It is globally agreed that Wi-Fi enabled handsets are much more than the ones that can support 802.1x/EAP. Although some of them support Extensible Authentication Protocol (EAP), most of the Wi-Fi networks still use IEEE 802.11 except the enterprise networks. Thus, our solution describes a way to improve IEEE 802.11 authentication.

There were no significant improvements in generic WLAN access as far as the security in initial authentication is considered. More specifically, there is lot of doubt about the existence of OSA which is considered to be a pre-RSNA authentication process and not acceptable anymore in contemporary wireless networks. The solution of piggybacking authentication information onto association Request/Response messages is also proposed. Finally, another proposal was to append the upper layer information on association Request/Response messages in order to speed up the link establishment process.

In our opinion, the first solution is promising with response to the authentication delay and more or less should be incorporated in the next standard. The only reason that OSA still exists is the backward compatibility with IEEE 802.11 state machine [8]. The second solution seems capable of improving the whole authentication process, though it does not seem to provide a fine grained and performance-wise acceptable solution towards more effective authentication. Finally, the third solution does not really improve the authentication process itself; rather, it is an intermediate approach to accelerate the link establishment delay. By the time mentioned, WEP and WPA security was already broken [9]. Consequently, there is a demanding requirement for security in contemporary wireless networks. Despite that, EAP authorization framework is not in the scope of this paper.

## III. Weaknesses and challenges of WEP, WPA and WPA2/IEEE 802.11

WEP and WEP2 use respectively 40 and 128 bit length keys with RC4 for encryption and CR4 for decryption. The length of the Initial Vector (IV) was also increased from 24 bits to 128 bits together with the key size. Using our test setup, we evaluated the authentication delay of WEP and WEP2 and figured-out the corresponding mean authentication delays; i.e. 9.35ms<11.84ms. WEP has several security issues, such as weak key usage, reuse of initial vectors, exposure to replay and packet forging and problems with the encryption algorithm. Other than that, key management and updating is poorly designed in WEP. These keys are weak and can be cracked, even in few hours or minutes using freely available software. The ability to modify packets, even without knowing the encryption key allows an attacker to modify or alter packets undetectably.

WPA was introduced to solve the problems of WEP without changing the existing hardware. WPA keys can go up to 256 bits, but not transmitted over the air to protect against packet monitoring. Compared to RC4 encryption, TKIP encryption allows better message security with the assistance of Message Integrity Check (MIC) [8]. This avoids packet forging and removes replay attack by utilizing a new IV sequencing discipline. Meantime, re-keying mechanism invalidates reusing encryption and integrity keys by an attacker to decrypt the messages. Due to the weakness of encryption algorithms, WPA is vulnerable to key-stream recovery attack and message falsification. WPA2 in other words is vulnerable to Denial of Service (DoS) attacks, such as data flooding, frequency jamming and Layer 2 session hijacking. Additionally, the control packets are not protected and open to DoS attacks. Weak authentication for control frames makes the MAC addresses are possible to be spoofed. However, WPA and WPA2 provide considerably good security in today's wireless networks eventhough they were already cracked.

## IV. An efficient approach to FIA; HIP-WPA

HIP-WPA is a light-weight authentication and key management protocol on 802.11 wireless networks. HIP-WPA utilizes HIP as a key management scheme which was initially designed to provide end-to-end authentication and key establishment. HIP introduces a new namespace for host identifiers. Thus, host identity can be represented either by a Host Identifier (HI) or by a Host Identity Tag (HIT). HI is the public key of an asymmetric key-pair. However, HI is not suitable to serve as a packet identifier since the length of the public key can vary. HIP Base Exchange (HIP-BEX) uses a Sigma-compliant 4-way handshake in order to establish a Diffie-Hellman (DH) key exchange and a pair of IPsec Encapsulated Security Payload (ESP) Security Associations (SAs) between two entities; the Initiator $(I)$ and the responder $(R)$ [10].

HIP-DEX; a diet version of HIP-BEX, does not apply any cryptographic hash on the HI. Instead, it uses the left 96 bits of an Elliptic Curve HI, the 4 bits of the HIT suite and the HIP IPv6 prefix. HIT is used to represent an identity. HIP traffic uses IPsec in ESP transport mode. Therefore, it can provide end-to-end encryption over IPsec ESP SAs. Note that the SAs are bound to HITs and thus, dynamic change of IPs can be handled without disconnecting the sessions.

Current 802.11 authentication techniques do not fit into today's constrained applications, especially when mobility comes into play. SAs built on top of HITs do not depreciate even if STA move between BSSs. By analyzing the experimental results, allowable incoming rate to an AP with WEP, WEP2, WPA and WPA2 are found to be 106, 84, 9 and 10 STAs/s. Results depict that older initial authentication solutions are faster. The attempts to strengthen security have increased the delay in authentication. To comply with the today's mobility requirements, we introduce our novel approach of FIA; a combination of OSA and HIP-DEX.

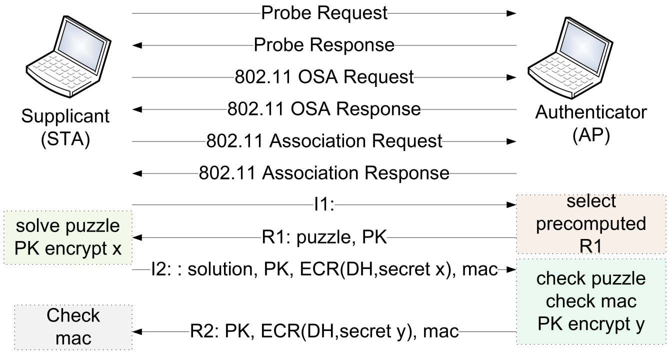
Probe Request
Probe Response
802.11 OSA Request
802.11 OSA Response
802.11 Association Request
802.11 Association Response
Supplicant (STA)
Authenticator (AP)
I1:
select precomputed R1
solve puzzle PK encrypt x
R1: puzzle, PK
I2: : solution, PK, ECR(DH,secret x), mac
check puzzle check mac PK encrypt y
Check mac
R2: PK, ECR(DH,secret y), mac

Fig. 1. HIP-WPA for initial authentication.

As shown in Figure 1, our routine starts with a probe request which is sent to scan the APs in the range. Probe response message delivers the AP's capabilities. When an AP is found, the mobile STA initiates OSA that accepts or rejects it to the AP. During the association phase, AP allocates the resources and synchronizes with the STA. Followed by the association, actual Authentication and Key Management (AKM) are initiated by sending an $I_1$ which triggers HIP-DEX. The AP replies with an $R_1$ packet by concatenating a cryptographic challenge and the algorithms it can support.

The replying $I_2$ message includes the solution to the challenge and a DH key wrapper that carries a key, i.e. one half of the final session key. At this point, if a password authentication is configured, the STA performs the appropriate actions in order to attach an authentication response with the $I_2$ message which is MACed by the STA. The $R_2$ packet contains a DH key wrapper that contains the other half of the final session key. HIP introduces an additional parameter which is a CMAC based message authentication code to authenticate $I_2$ and $R_2$ frames.

As it is stated in [11], DEX is equivalent to 802.11 Master and Pair-wise Transient Key (PTK) generation, though it is handled in a single exchange in DEX. HIP-DEX establishes two SAs. The first one for the DH derived key (Master key equivalent) and the other one for the session key (PTK equivalent). The DH key is used to secure DEX parameters and to authenticate the HIP packets [11]. The session key is used for authentication and securing the traffic. HIP-DEX reduces both message and computational overhead. This approach is lightweight by the use of Elliptic Curve (EC)-based public key cryptography. The HIP-DEX protocol forfeits signatures and hash functions from the security parameter negotiation and uses CMAC for message authentication. In a nutshell, these changes are expected to lead to a reduction of CPU utilization and improvement in authentication security.

One of the main advantages of HIP is the ability to fit directly into the 802.11 key model(MK, PTK, Group-wise Transient Key (GTK)). The first thought about integrating HIP into such a process is to let HIP datagram to run over 802.11 authentication frames [12]. GTK could be delivered on an association response frame as a reply to an association request frame which contains a HIP-UPDATE datagram. The HIP-UPDATE can generally act as a re-keying mechanism when needed. The above scheme introduces a much simpler architecture and seamless handovers within the same ESS. More specifically the established HIP-DEX SAs are preserved during handovers within the same ESS as the SA establishment is valid between the mobile STA and AP. The procedure should be rather simple. According to Figure 1, the basic steps are:

- The APs transmit beacon frames that advertise the HIP capabilities of the network as well as the STA's address (alternatively the mobile STA could perform active scanning and begin a HIP message exchange to responder's link-local address or pre-defined multicast address [3]).
- The STA performs standard Open System Authentication and Association.
- The STA (acts as Supplicant) starts a DEX exchange with the AP (acts as Authenticator).
- The STA and AP perform HIP-DEX and exchanges the keys.
- Seting-up ESP SAs.
- Flow of ESP protected traffic (no HIP overhead).

This approach would support initial authentication of tens of APs. However, in the case of ESS transition, a HIP based mobility solution should also be designed. Mobility may include re-keying and should use the HIP-UPDATE message in order to inform the peers about the change of IPs. Compared to the current IEEE 802.11 initial authentication techniques, the HIP-WPA solution seems to be efficient. In terms of exchanged data, HIP-DEX needs no more than 550 bytes to complete the key exchange. Table I summarizes the DEX message lengths.

Considering each and every DEX message is encapsulated into an authentication frame (approximately 40 bytes) makes a total of 542 bytes to complete 4-way handshake.

TABLE I
MESSAGE LENGTHS OF HIP-DEX

| Message | Length (bytes) |
|---|---|
| $I_1$ | 40 |
| $R_1$ | 92 |
| $I_2$ | 148 |
| $R_2$ | 102 |

On the contrary, a WPA2 operation may require the exchange of up to 1300 bytes until the whole AKM process is completed. Although, this number may fluctuate depending on the used WPA2 security specific mechanisms, the advantage of this solution is the seamless BSS handovers and the significantly low overhead that DEX poses on the wireless controller during the ESS transitions. DEX certainly promises the reduction of authentication delay, not to mention the seamless transitions during BSS handovers. As it was explained, these are valid reasons to believe that DEX can provide delay which can be tolerated by most of the delay sensitive applications.

## V. Implementation

There are already two implementations of IEEE 802.1x that are presented in [13] and [14]. We have chosen [13] which provides couple of different options for initial authentication. The implementation consists of massive amount of code lines which are interconnected and difficult to analyze. The supplicant and the authenticator have the following configurations. Supplicant with an i5 CPU of 2.67GHz and authenticator with a CPU of 2.16GHz and both running 2.6.35 Linux kernel. The authenticator has an Atheros AR5001X+ wireless network adapter and the supplicant is equipped with an integrated wireless network adapter.

The wireless control unit of the supplicant is implemented with wpa_supplicant module which is responsible for key negotiation between the supplicant and the authenticator. Wpa_supplicant is designed to be a “daemon” program that runs in the background and acts as a back-end component which controls the wireless connection [13]. Respectively, authenticator uses the hostapd module [13] which is also a “daemon” program. These modules share a common set of codes. By default, wpa_supplicant module periodically scans for available networks and connects once the requested Service Set Identification (SSID) is found. Legacy WLANs network discovery may take more than 2s in average [15].

The authenticator is configured with a static channel number, whereas the supplicant scans all the channels until it detects the correct SSID. Channel configuration is important when supplicants use fast inter-AP transition. IEEE802.11r can reduce delay at least in transition between the APs. But, either 11r or 11i does not address the actual problem of initial authentication. On the other hand, time synchronization between STAs and APs in the same BSS would take up to 2 ms which is counted to the total authentication delay. Attempts to minimize this delay require modifications in the driver level that also implicate some reinforcements in 802.11 amendment. Thus, our work is focused in minimizing the delay in protocol level attachment that goes through several phases, such as authentication, association, key-generation and exchange.

In any authentication scheme, the most time-consuming process is the AKM. Thus, the developers’ main focus over AKM should be to reduce the latency which results to suppress the overall delay in 802.11 without weakening the security aspects or over-utilization of CPU. HIP-DEX is a secure AKM scheme that fits into many constrained applications, due to enhanced security it provides with Elliptic Curve Cryptography (ECC) and comparatively less overhead [16]. The HIP-DEX module was developed in C++ with the support of OpenSSL version 1.0.1c which includes ECC point multiplication for ECDH handshake [17].

Wpa_supplicant and hostapd were developed in C and include several C language specific data types and method overloading techniques. Authenticator and supplicant are configured with static IPs before the applications are executed independently. Finally, the total delays in different approaches were measured; given the fact that all management frames were transmitted in 1 Mbps mode. Hence, the delays include link-layer establishment (authentication and association) and AKM times.

HIP-WPA solution consists of two phases; i.e. link-layer establishment and secure AKM with HIP-DEX. OSA is a part of link-layer establishment which is a default authentication mechanism for pre-RSNA equipments. OSA utilizes a single exchange which takes about 1.2 ms according to the experimental results in Figure 2. A STA and AP must complete IEEE 802.11 authentication prior to the association, though it is not mandatory in an independent BSS. However, we propose OSA in conjunction with HIP-WPA for backward compatibility with pre-RSNA devices.

## VI. Experimental Results

On our test setup, we have implemented couple of commonly used IEEE 802.11 initial authentication mechanisms and measured authentication and association delays independently with Wireshark traces [18]. Figure 2 depicts the measured WEP and WEP2 delays. WEP2 extends the IV and key values to 128 bits in an effort to fight against brute-force attack and duplicate IV deficiency. This slightly increases the authentication delay in general though; both WEP and WEP2 use the same 802.11 association followed by the successful authentication. Results indicate 9.35 ms mean delay for WEP and 11.84 ms mean delay for WEP2. This indicates, more advance security features would consume more CPU cycles for cryptographic operations in general. As a consequence, WEP2 consumes more time than WEP in authentication.

Figure 3 presents a delay analysis of WPA and WPA2. Either WPA or WPA2 is much more secure than WEP or WEP2, because they utilize pass-phrases (supplied by the user)

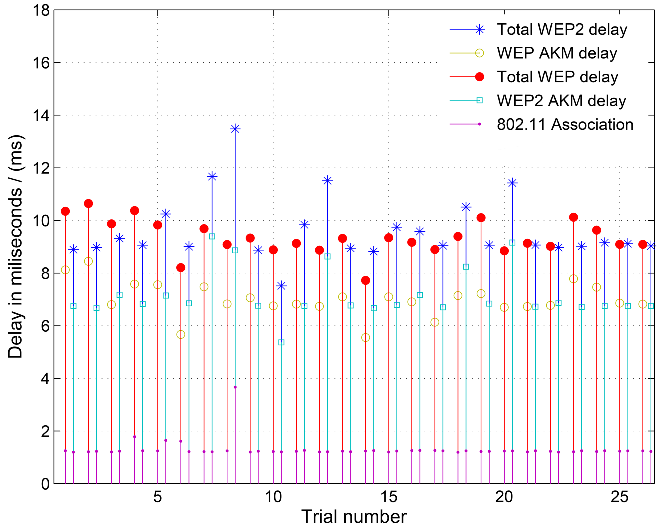

Fig. 2. WEP based initial authentication: a delay analysis.

as well as shared keys that make WPA or WPA2 even harder for an attacker to break. Almost all small Wi-Fi networks that need sustainable level of security without an extra cost or more complex configurations use WPA (i.e. mostly home and office networks) though they do not comply with the requirements of modern real-time applications, such as VoIP.

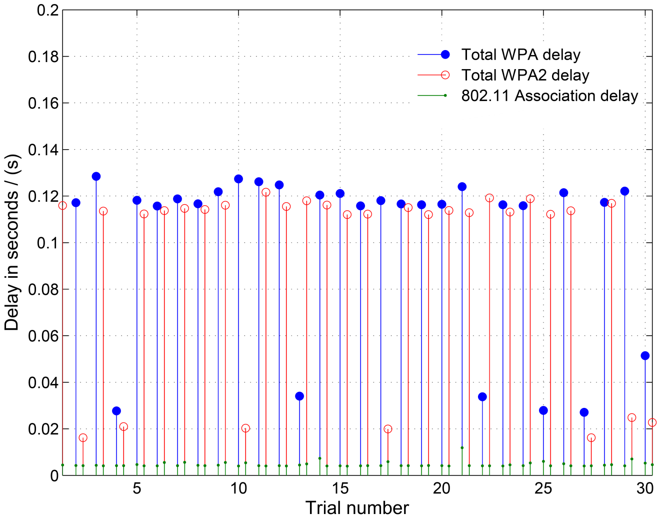

Fig. 3. WPA based initial authentication: a delay analysis.

WPA2 is developed on top of RSN framework, which provides support for all WPA mechanisms, including Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption based on AES ciphering (128 bit key in our case) as an alternative to TKIP in WPA. AES lowers the complexity in message encryption and thus, it also reduces the authentication delay. More specifically, the mean authentication delay for WPA is measured to be 0.103 s and 0.093 s in the case of WPA2. As of ITU-T G.114, VoIP applications demand the maximum affordable one-way latency of 0.15 s. Since, the previous results include the entire voice path, those networks should have a transit latency which is considerably less than 0.15 s. Thus, either WPA or WPA2 would not fit into today's real-time applications such as VoIP.

The challenge now is to reduce the authentication delay while maintaining a sustainable level of security. Meantime, the demand of security is increasing as a result of developing computer knowledge in local society. HIP-WPA is a solution where the latter requirements exist in a single protocol. ECC based protocol design reduces the delay and introduces an unbreakable level of security [19]. Our implementation allows us to measure the mean delay of HIP-WPA (0.0305 s) which is more than 300% of improvement compared to WPA2. This also complies with the delay requirements of any VoIP service. Figure 4 presents an overall comparison of couple of 802.11 techniques that we have discussed so far. However, it depicts the fact that our HIP-WPA is promising solution compared to other existing 802.11 solutions.

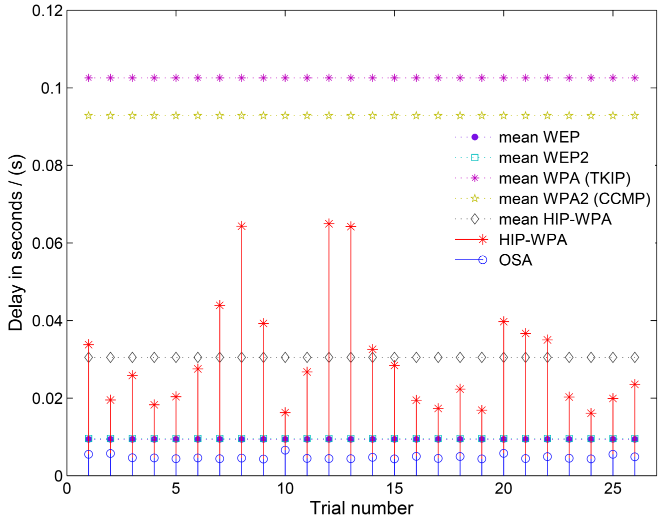

Fig. 4. HIP-WPA and overall analysis of FIA solutions.

## VII. Security Considerations

Though HIP does not directly address the problems of privacy and accountability; they are provided in other means. The use of cryptographic identities are self-certified, thereby provides automatic identity authentication. Separation of identities and locators makes it is easier to hide the topological location from the attackers. The privacy extensions of HIP allow to hide the identities from the third party network entities in a commercial network. HIP also extends the support for secure signaling delegation.

That, in turn, can be used to implement application-level service delegation and subnet mobility. The idea behind the cryptographic delegation is simple but powerful. HIP-DEX uses the same puzzle mechanism as BEX to protect the responder from packet DoS attacks. It also protects the hosts from replay attacks by using puzzle as a nonce and CMAC to generate ECDH. HIP-DEX uses AES encryption to protect being eavesdropped and ECDH to mitigate spoofing and Sybil attacks. However, passive attacks such as HIT spoofing have limited effect depending on how often the initiator communicates to the spoofing responder.

On the other hand, the same HIP-WPA approach can be improved to enable the mobile router scenario which is a diversification of network mobility. Such a scenario is comparatively more vulnerable to security attacks due to frequent associations and disconnections that leave more opportunities to an attacker. HIP-WPA does not reuse the keys and thus, maintain the security level over the transitions. Though, HIP-DEX does not support perfect forward secrecy, BEX integration would remove reauthentication by eliminating the unnecessary exchanges.

## VIII. Discussion

The current 802.11 solutions, such as WEP, WPA, and WPA2 are already broken and thus, do not provide enough security in authentication. Hence, the need of secure initial authentication is a critical requirement in wireless access. Major disappointment in WLAN is the undesirable initial authentication delay that takes up to several seconds in many cases due to scanning, synchronizing, IP acquisition over DHCP, etc. As of 802.11 amendment, authentication is a pre-request for association though OSA is not an essential exchange in terms of security.

Therefore, excluding this exchange would be preferred, since it does not provide expected security in authentication. But, 802.11 standards do not allow this by the definition of the state machine. Attempts to skip OSA, push the station back to "unauthenticated, unassociated" state without moving towards the next state. Hence, excluding OSA needs some modifications in the flow of 802.11 state machine as well. We recommend this is desirable in the next amendment that sets path for independent implementations. Finally, we allow OSA for backward compatibility with 802.11 standards. It is also possible to piggyback the first and second OSA messages in $I_1$ and $R_1$ which will reduce the delay by one round-trip.

## IX. Conclusion

In this paper, we have presented an alternative solution for FIA, namely HIP-WPA which is based on HIP-DEX. Our attempt is to combine the features of HIP-DEX with traditional OSA. HIP-WPA allows for lot of benefits as far as the mobility and security are considered. We believe that intra-network handovers (BSS transitions) can be made much faster and the inter-network ones (ESS transitions) are quite "cheap" in terms of cost as DEX allows a light AKM overhead. More specifically, the authentication delay can be reduced by three times or by 300% (0.0305s) compared to WPA2 thanks to the reduced length in authentication exchange (about 550 bytes).

Therefore, HIP-WPA can be used for delay sensitive applications that are not complying with WPA (0.103s) or WPA2 (0.093s). However, there are some security considerations that should be reviewed like the strength of the derived keys and the lack of perfect forward secrecy for advance mobility and security requirements.

## Acknowledgment

This work has been performed in the framework of the CELTIC project CP7-011 MEVICO. The authors would like to acknowledge the contributions of their colleagues. This information reflects the consortiums view, but the consortium is not liable for any use that may be made of any of the information contained therein.

## References

[1] T. Henderson, J. Ahrenholz, and J. Kim, "Experience with the Host Identity Protocol for Secure Host Mobility and Multihoming," in *IEEE Wireless Communications and Networking*. IEEE, 2003, pp. 2120–2125.

[2] J. Arkko, P. Eronen, and H. Tschofenig, "Quick NAPSecure and Efficient Network Access Protocol," in *in Proc. 6th International Workshop on Applications and Services in Wireless Networks*, 2006, pp. 163–170.

[3] J. Korhonen, A. Mkela, and T. Rinta-aho, "HIP Based Network Access Protocol in Operator Network Deployments," *in First Ambient Networks Workshop on Mobility, Multiaccess, and Network Management*, pp. 35–59, 2007.

[4] P. Nikander, A. Gurtov, and T. Henderson, "Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks," *Communications Surveys & Tutorials, IEEE*, vol. 12, no. 2, pp. 186–204, 2010.

[5] S. Novaczki, L. Bokor, and S. Imre, "A HIP Based Network Mobility Protocol," in *Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on*. IEEE, 2007, p. 48.

[6] A. Gurtov, "Host Identity Protocol (HIP): Towards the Secure Mobile Internet," *Wiley Publishing*, 2008.

[7] Morioka, H. . (2010) Feasibility Study of FIA. . [Online]. Available: https://mentor.ieee.org/802.11/dcn/10/11-10-0836-01-0fia-feasibility-study-of-fia.ppt

[8] "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," tech. rep., Dec. 2007., Tech. Rep.

[9] E. Tews and M. Beck, "Practical attacks against WEP and WPA," in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 79–86.

[10] A. Gurtov, "Host Identity Protocol (HIP): Towards the Secure Mobile Internet," *Wiley Publishing*, p. 332, 2008.

[11] R. Moskowitz, "HIP Diet EXchange (DEX) draft-moskowitz-hip-rg-dex-04," Internet Engineering Task Force,Status: Work in progress, Tech. Rep.

[12] Moskowitz, R. (2010) Summary and Comments, FIA Security Analysis. [Online]. Available: https://mentor.ieee.org/802.11/dcn/10/11-10-0980-00-0fia-fia-security-analysis-bobm.pptx

[13] J. Malinen. (2012) Developers' documentation for wpa_supplicant and hostapd. [Online]. Available: http://hostap.epitest.fi/wpa_supplicant/devel/

[14] A. Mishra, D. Payne, C. Hessing, and T. Simons. (2010) Open1X, IEEE 802.1X Open Source. [Online]. Available: http://open1x.sourceforge.net/

[15] W. Lim, D. Kim, Y. Suh, and J. Won, "Efficient WLAN Discovery Schemes Based on IEEE 802.21 MIH Services in Heterogeneous Wireless Networks," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008, pp. 1–5.

[16] S. Namal, J. Pellikka, and A. Gurtov, "Secure and Multihomed Vehicular Femtocells," in *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*. Yokohama, Japan: IEEE, May 6-9 2012, pp. 1–5.

[17] M. Cox, R. Engelschall, S. Henson, B. Laurie *et al.*, "The openssl project," 2002.

[18] G. Combs *et al.*, "Wireshark," *Web page: http://www. wireshark. org/last modified*, pp. 12–02, 2007.

[19] P. Nie, J. Vähä-Herttua, T. Aura, and A. Gurtov, "Performance analysis of HIP diet exchange for WSN security establishment," in *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks*. ACM, 2011, pp. 51–56.