Emulation of Secure Wi-Fi Communication: A Performance Gap Analysis against a Virtual Test-bed

Simone Soderi[†], Harri Viittala[‡], Jani Saloranta[‡], Alessandro Mancini[†]
Matti Hämäläinen[‡], Jari Iinatti[‡]
[†]GE Transportation Systems, Florence, Italy. email:simone.soderi, alessandro.mancini1@ge.com
[‡]Centre for Wireless Communications, University of Oulu, Oulu, Finland email:firstname.lastname@ee.oulu.fi

***Abstract*—Wireless local area networks (WLANs) gained ever-growing importance in public transportation systems where they are selected to reduce installation costs and introduce new services. However, the introduction of a wireless interface in safety critical applications implies different communication protocol analysis and the introduction of a security layer is indispensable to implement defenses from malicious attacks. Host Identity Protocol (HIP) based network with IPSec is the network architecture proposed to secure wireless communications in large public transportation system. This paper analyses a comparison between the proposed architecture tested in a real environment and in an emulated scenario. The measurement campaign was carried out in outdoor using commercial on the shelf (COTS) Wi-Fi devices. The Common Open Research Emulator (CORE) with the Extendable Mobile Ad-hoc Network Emulator (EMANE) framework were used to evaluate the same scenario in a virtual test-bed. Results indicate how the end-to-end secure wireless communication built in the emulator works similarly to an intra-vehicular on-board network.**

***Index Terms*—Emulator; HIP; Security; Vehicle; Wireless.**

I. Introduction

Wi-Fi communications have a primary role in wireless networks because of their wide range of applications. Nowadays wireless local area networks (WLANs) provide the needed connectivity in public transportation systems (e.g., urban-transit, railway, mining and articulated buses), auto industries (e.g., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and intra-vehicular communications). Many of these systems require high level of safety with more complex development and testing processes. Specific standards have to be applied for the design of safe systems. The IEC 61508 [1] requires hazards and risks analysis in order to reduce or mitigate issues making the residual risk acceptable. This standard defines four ranks of Safety Integrity Levels (SIL). Each level states the amount of risks reduction in order to guarantee the degree of reliability of the system. SIL is relative to the single function and not to the entire plant. A system will have several functions and each of these has the associated SIL. The massive usage of wireless communications in industrial fail-safe applications introduced advantages but on the other hand imposed a different network architecture analysis in order to consider safety and security. Safety avoids physical harm to humans and things whereas security applies defenses from malicious attacks [2]. Now services carried out by WLAN combined with the increasing complexity of networks need to have appropriate tools to facilitate a rapid assessment of feasibility and have an useful indication of the expected performances. The use of WLAN for cable replacement [2] is an attractive solution in terms of costs reduction, maintainability and scalability. This paper presents a gap analysis study between an emulated wireless communication and end-to-end WLAN outdoor link. The main role of cyber-security and flexibility offered by a network emulator have shown that the proposed scenario offers many benefits in terms of rapid network prototyping giving also a valid support to test unconventional security protocols.

The paper is organized as follows: Section II overviews differences between simulators and emulators. Section III introduces the security for V2V and V2I communications. The security architecture tested is described in Section IV where are also compared outdoor measurements and virtual test-bed. Finally Section V presents results and Section VI concludes the paper.

II. Related Work

Studies in literature (e.g., [3], [4]) describe in detail simulators and emulators as useful tools during the performance evaluation for wireless networks. First, the difference between simulations and emulations should be clarified. A simulator behaves similarity to the original system with a completely different implementation. Models carried out by simulations may not be as accurate as real implementation. Nowadays there are many general purpose network simulators and among the most popular of these are:

- OPNET (Optimum Network Performance) is a computer software to simulate communication networks [5];
- OMNET++ (Objective Modular Network Testbed in C++) is a discrete event simulation tool designed to simulate

Project co-funded by the Tuscany Region and European Community under the 2007-2013 POR CREO FESR program.

978-1-4799-0846-2/13/$31.00

computer networks [6];
- TOSSIM (Tiny Operating System Simulator) simulates entire TinyOS applications [7]. TinyOS is an open source operating system for low-power wireless devices;
- NS-3 (Network Simulator 3) is a discrete event network simulator [8].

An emulator reproduces exactly external behavior of the system being emulated. It is a replica of the original system but works in a different environment. Moreover, the emulator supports all the functionality and is binary compatible with the emulated system. Basically emulators are hybrid choice in order to achieve more accurate results than simulators when the real deployment of the emulated system is not possible [4], e.g., wireless communications in laboratory. Emulators which by their nature are closer to the specific application must be chosen according to what would be modeled, e.g.,

- CORE (Common Open Research Emulator) is a tool for building virtual networks [9];
- EMANE (Extendable Mobile Ad-hoc Network Emulator) is a framework for real-time modeling of mobile network systems [10].

CORE (e.g., [3], [9]) implements virtual network stack and name-spaces for protocols and applications emulating network layer (i.e. layer 3) and upper layers (i.e. transport, session, application). On the other hand EMANE provides physical (PHY) and media-access-control (MAC) models in order to emulates layers 1 and 2.

The experience described in this paper combines CORE with EMANE in a virtual test-bed for network emulations. The CORE architecture includes a *CORE daemon* to manage emulation sessions and a graphical user interface (*CORE GUI*) to control the emulation. Finally CORE provides a Python framework for building networks using *CORE Application Programming Interface (API)*. Through Python scripts CORE allows the possibility of building the virtual wireless networks (e.g. Figure 1) running specific protocols.

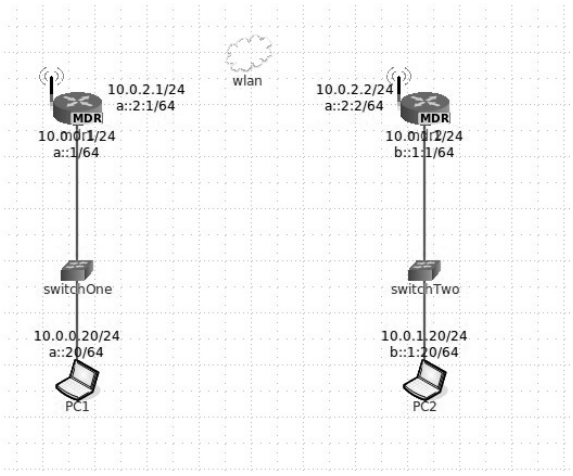

Fig. 1. End-to-end communication with CORE/EMANE

EMANE architecture consists of Network Emulation Modules (NEMs). These are logical components with the capabilities to emulate a particular type of network technology. Each NEM consists of three components: PHY Layer, MAC Layer and Transport. These components are connected through a bidirectional cross-layer communication. When a packet is sent down to the network stack, the PHY layer sends data to Over-The-Air (OTA) manager that emulates the multicast communications among NEMs.

III. Security Introduction of the V2V and V2I communications

Modern vehicles are controlled by complex distributed systems with a large number of processors, millions of lines of codes and physical interfaces [11]. For example an attacker embarked on the vehicle could launch intentional attack to the Wi-Fi on-board network taking control of breaks, lighting, steering or entertainment subsystem.

The extensive usage of WLAN in public transportation provide several advantages but on the other hand it adds special requirements to the network security. V2V and V2I are vulnerable to the following most common types of attacks:

- authentication falsified: Man in the Middle (MitM);
- information disclosure: snooping, sniffing and eavesdropping;
- system availability: Denial of Service (DoS);
- connection integrity: replay.

Normally wireless communications in fail-safe system transfer sensitive information and may be really attractive for many attackers. These wireless communications include security services, e.g., authentication, confidentiality, integrity and availability. In the following, a set of possible attacks to these security services is given as example [12].

Confidentiality attack: unauthorized interception of private information. This attack damages the privacy leaving intact the confidential data (e.g., eavesdropping and MitM).

Integrity attack: modification of data in transit over the wireless network in order to mislead the receiver or facilitate another attack (e.g., DoS, 802.11 data replay and frame injection).

Authentication attack: stealing of user identifies and credentials in order to gain the access to the network (e.g., WPA/WPA2-PSK cracking and application log-in theft).

Availability attack: denying legitimate users to access WLAN resources (e.g., Queensland DoS and 802.11 beacon flood).

IV. Secure Architecture Tested

Host Identity Protocol (HIP) based network combined with a tunnel technology was the architecture proposed in [13] and [14] to secure wireless communications in public transportation systems against DoS and MitM attacks. HIP allows the separation between the identification and localization information that normally comes with the IP address.

HIP introduces the *host identity layer* in the TCP/IP stack between networking and transport layers, as specified in

RFC5201 [15] by the Internet Engineering Task Force (IETF). HIP establishes a Security Association (SA) between hosts via a four way handshake protocol named Base Exchange (BEX). When SA succeeds hosts uses IP Security (IPSec) Encapsulating Security Payload (ESP) to exchange data through a secure tunnel.

IPSec [16] provides three different implementations:

1. IPSec protocol and its capabilities are directly integrated into the IP protocol, without any extra hardware or additional layers;
2. Bump In The Stack (BITS) inserts an extra layer (i.e. IPSec) between IP and Data-link layer with the intent to provide security for each packet;
3. Bump In The Wire (BITW) architecture adds an external device that provides IPSec services intercepting outgoing datagrams.

These architectures are supported by IPSec with two basic modes of operation: *transport mode* for IPSec integrated solution and *tunnel mode* for BITS or BITW.

The proposed architecture tested in real outdoor measurements and emulated in CORE/EMANE considered HIP with IPSec integrated into the IP protocol (i.e. transport mode). In this case HIP handles the keys exchange protocol and IPSec sets up the secure tunnel between two end-points. During field trials and emulations OpenHIP was selected because it is an open source with Berkley Software License (BSD) [17].

V. SCENARIO

A. Virtual test-bed

The end-to-end communication presented in the virtual test-bed (i.e. CORE/EMANE) is shown in Figure 1. This section describes the PHY and MAC configurations of NEMs used to emulate secure Wi-Fi communication. EMANE provides an Universal PHY layer with the following capabilities [10]:

- Pathloss calculation: the pathloss value is calculated in real-time based on the selected channel model. There are three different channel models: *freespace*, *2ray* and *pathlossmode* (i.e. custom defined pathloss);
- Receiver power calculation;
- Custom antenna pattern;
- Noise processing: ability to adjust the noise floor emulating the impact of intentional or unintentional noise sources.

CORE emulates wireless networks using pluggable PHY and MAC models available in EMANE. These models are configured through the *CORE GUI*. CORE's WLAN configuration dialog has all the parameters to control the wireless virtual node (e.g., center frequency bandwidth, channel bandwidth, antenna gain, antenna azimuth, antenna elevation, transmitted power, 802.11 a/b/g mode and data rate). The interface between CORE and EMANE is the TAP device [9].

As a first approximation of LOS outdoor communication the freespace channel model was selected. In the far field region the signal strength loss in decibel [dB] is given by

$$PL = 32.44 + 20 \cdot log(f) + 20 \cdot log(d), \quad (1)$$

where f and d are the frequency [MHz] and the range [km] respectively.

For each received packet the Universal PHY layer implemented in EMANE calculates the received power [dBm] as

$$rxPower = txPower + txAntennaGain + rxAntennaGain - PL, \quad (2)$$

where *txPower* is the transmitted power [dBm], *txAntennaGain* is the transmitted antenna gain [dBi], *rxAntennaGain* is the receiver antenna gain [dBi] and *PL* is the freespace pathloss [dB].

In terms of antenna gain, the Universal PHY layer allows to utilize custom radiation pattern specified via XML file. This functionality gives plenty of freedom to antenna gain definition as function of elevation, azimuth and NEM's orientation. The vehicular directional antenna selected for outdoor measurements was affected by up-tilt phenomenon as shown in Figure 2. However the beam up-tilt, around 15 degrees, was considered via XML file and utilized during the emulation experiment.

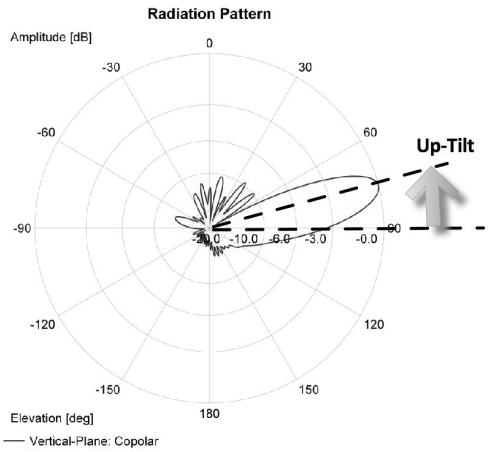

Fig. 2. Up-tilt phenomenon on directional antenna.

B. Link Budget

The emulator PHY layer receives packets based on the evaluation of the signal-to-interference-plus-noise-ratio (SINR). The ability of a node to receive data depends on its location in the emulator scenario (i.e. canvas). Other key factors that affect the SINR are: pathloss model (i.e., 2ray, freespace), intentional or unintentional interference signals and receiver sensitivity.

The *Receiver Sensitivity* [dBm] is given by

$$rxSensitivity = -174 + NF + 10 \cdot log(BW), \quad (3)$$

where *NF* and *BW* are the Receiver Noise Figure [dB] and Receiver bandwidth [Hz] respectively. The SINR is described by the general expression

$$SINR = rxPower - NoiseFloor. \quad (4)$$

The overall *Noise Floor* for a given receiver combines Radio Frequency (RF) interference and receiver sensitivity. In the end-to-end wireless communication for each node there is no other interference and the SINR can be put into the simple form

$$SINR = rxPower - rxSensitivity. \quad (5)$$

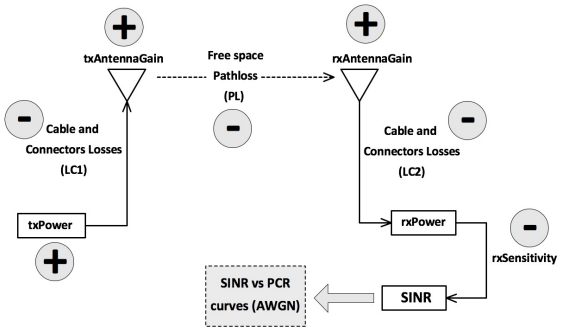

Fig. 3. Positive and negative contributions in the link-budget

Figure 3 shows positive and negative contributions in the end-to-end wireless communication. To compare outdoor scenario (Figure 4) with the same emulated network (Figure 1) a link budget was prepared. Considering the cable and insertion losses (i.e. *LC1* and *LC2*), (4) becomes

$$SINR = rxPower - rxSensitivity - LC1 - LC2. \quad (6)$$

The IEEE802.11abg EMANE model uses packet-completion-rate (PCR) curve tables to produce a probability-of-reception (POR) from a given SINR value. PCR is given by

$$PCR = (1 - BER)^L, \quad (7)$$

where *L* is the packet length and *BER* is the bit error rate.

EMANE provides as default BER curves for an additive-white-Gaussian-noise (AWGN) channel and these were used in the experiment discussed.

C. Outdoor Measurements

The simulated scenario was benchmarked against an end-to-end outdoor wireless communication between two nodes. The measurement campaign was carried out near Oulu (Finland) in an open area selected in order to have line-of-sight (LOS) till to 800 m. Each node was composed of one embedded Linux PC with one Wi-Fi module compliant with IEEE standard [18], cables (i.e. Ethernet, coaxial) and one adjustable heights stand. On the stand, a metallic plate was installed to support antennas (Figure 4). Iperf tool was run from the Linux PC in each node to profile the communication transmitting and receiving UDP traffic for different distances. Table I presents the most important wireless parameters. For each distance the average of 180 s of transmission time was measured for throughput, jitter and packet loss.

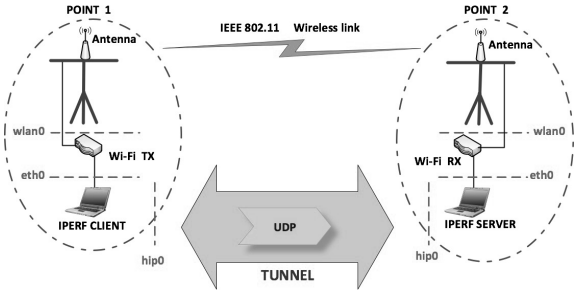

Fig. 4. Field trials outdoor scenario

TABLE I
WIRELESS LINK PARAMETERS

Parameter	Value
Radio protocol	802.11 g
Wi-Fi channel	9 (2452 MHz)
Transport protocol	UDP
Security protocols	HIP
EIRP[1]	20 dBm[2]
Traffic bandwidth	10 Mbps
802.11 Channel bandwidth	20 MHz
Antenna Type	Directional[3,4], Omni-directional[4]
Directional Antenna Gain[2,3]	14.5 dBi
Omni-directional Antenna Gain[3]	6 dBi
Antenna height	3 m
Distances in outdoor	250, 500, 700, 800 m
Distances in virtual test-bed	100, 250, 500, 550, 600, 700, 800, 900, 1000, 1050 m
Link type	LOS
Transmission duration	180 s

[1] Equivalent isotropic radiated power (EIRP).
[2] Maximum EIRP in EU at 2.452 GHz is 20 dBm.
[3] Used in the real outdoor measurements set-up.
[4] Used in the Virtual test-bed set-up.

VI. RESULTS

The main goal of this study was to develop a methodology to compare a security protocol in a virtual test-bed against same network topology implemented with COTS devices without jamming, security attacks and interference. Iperf tool was used to measure throughput, jitter and packet loss in both emulator and real scenario. In order to avoid fragmentation the UDP packet size was set to 1470 B in Iperf when the Maximum Transmission Unit (MTU) was 1500 B. By setting the packet size smaller than MTU the lost datagram rate correspond to packet loss rate. Each test run for 180 s.

The data rate during emulations in CORE/EMENE was 54 Mbps and the virtual wireless nodes (i.e. NEMs) automatically adjust over-the-air rate by themselves. Moreover NEMs used PCR/SINR curve defined via XML file for this specific data rate.

Table I presents ranges tested and till 500 m there are not significant difference between real measurement and emulated scenario as shown in Figure 5-Figure 7.

A. Virtual test-bed vs Outdoor Measurements

Both measurements cases (i.e. emulator and outdoor) were set up with EIRP = 20 dBm. Moreover the virtual scenario was configured with the same radiation pattern the antennas used in the experiment. For each side the emulation scenario considered 2 m coaxial cable with a cable loss of 0.5 dB/m and 0.5 dB as overall insertion loss. The Noise Figure was 4 dB as the real Wi-Fi module used and 5 dB of *implementation losses* were considered.

In the range between 250 m and 800 m (Figure 5) the emulator and outdoor scenario gave same performance in terms of throughput and packet loss. On the other hand jitter was larger with CORE/EMANE but the difference with the real measurements is always on the range of 0.5 ms. Curves in Figure 5 and Figure 7 do not shows an evident performance degradation when the security was introduced with the same trend for longer distances.

By increasing the range between nodes in the virtual scenario by 100 m the connection worked till 1050 m. After distance between two radios was over 950 m, throughput decreased with a significant increase of jitter and packet loss.

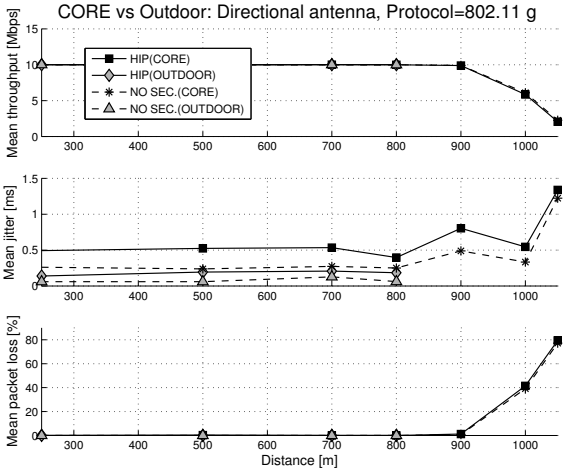

Fig. 5. Comparison between Virtual test-bed and real measurements.

B. Different antennas in the Virtual test-bed

An important feature of EMANE is its ability to use custom defined antenna radiation pattern via XML file. In this section a comparison between omnidirectional and directive antenna is presented (Figure 6).

As expected, also in the emulated network, directive antenna with gain equals to 14.5 dBi achieved longer ranges till 1050 m. Instead omnidirectional antenna did not get any connection over 600 m.

VII. Conclusion and Future Work

The HIP architecture was introduced as promising protocol for vehicular communications. The end-to-end communication presented in this experience works similarly to an intra-vehicular (i.e. same vehicle) on-board network.

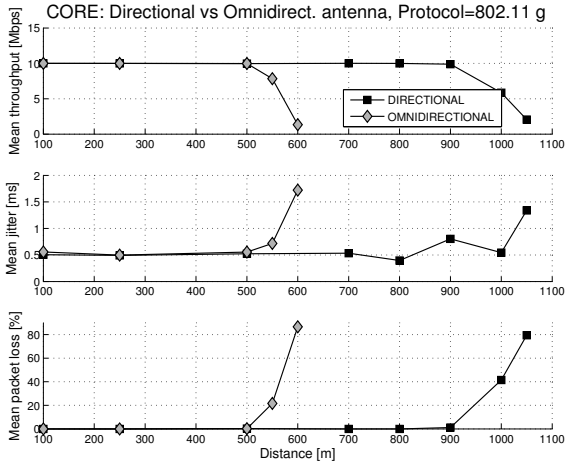

Fig. 6. Omnidirectional vs Directional antenna in the Virtual test-bed.

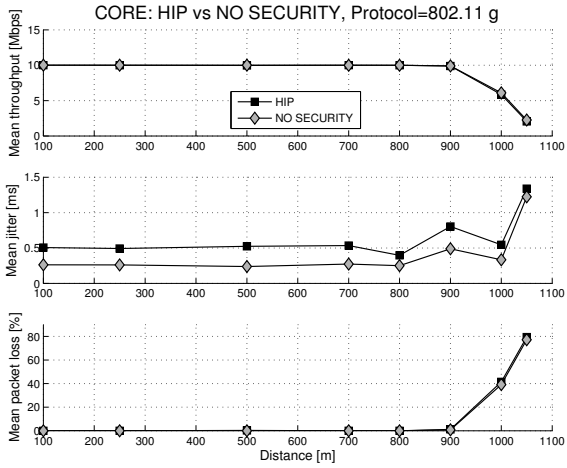

Fig. 7. Performance degradation with HIP in the Virtual test-bed.

CORE with EMANE were proposed as virtual test-bed and its performance were compared with a real scenario. Finally the usability of this emulator was demonstrated presenting throughput, jitter and packet loss performance against outdoor measurement for the proposed architecture (i.e. end-to-end outdoor wireless communication with HIP and directive antennas). Furthermore the reliability of CORE/EMANE offers an important tool to study security attacks without any other measurements campaign.

Modern vehicles are controlled by complex computer control systems with broad wired and wireless connectivity . The emulation tool presented could be the right framework to test vehicular threats models. CORE supports virtual emulation of PC, routers and switches. EMANE extends emulation at lower layers.

Future work could investigate network scalability performance and introduce nodes mobility in order to evaluate the HIP impact on a more complex vehicular network.

REFERENCES

[1] "Functional safety of electrical/electronic/programmable electronic safety-related systems," IEC 61508, April 2010.

[2] J. Gronbaek, T. Madsen, and H. Schwefel, "Safe Wireless Communication Solution for Driver Machine Interface for Train Control Systems," in *Systems, 2008. ICONS 08. Third International Conference on*, April 2008, pp. 208 –213.

[3] J. Ahrenholz, "Comparison of core network emulation platforms," in *Military Communications Conference, 2010 - MILCOM 2010*, 2010, pp. 166–171.

[4] M. Imran, A. Said, and H. Hasbullah, "A survey of simulators, emulators and testbeds for wireless sensor networks," in *Information Technology (ITSim), 2010 International Symposium in*, vol. 2, 2010, pp. 897–902.

[5] OPNET. [Online]. Available: http://www.opnet.com/

[6] OMNET++. [Online]. Available: http://www.omnetpp.org/

[7] TOSSIM. [Online]. Available: http://docs.tinyos.net/tinywiki/index.php/TOSSIM

[8] NS-3. [Online]. Available: http://www.nsnam.org/

[9] CORE. [Online]. Available: http://cs.itd.nrl.navy.mil/work/core/index.php

[10] EMANE. [Online]. Available: http://cs.itd.nrl.navy.mil/work/emane/

[11] Comprehensive Experimental Analyses of Automotive Attack Surfaces . [Online]. Available: http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[12] List of Wireless Network Attacks. [Online]. Available: http://www.brighthub.com/computing/smb-security/articles/53949.aspx

[13] D. Kuptsov, A. Khurri, and A. Gurtov, "Distributed user authentication in wireless LANs," in *World of Wireless, Mobile and Multimedia Networks Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*, June 2009, pp. 1 –9.

[14] IETF RFC5201 -Section 8. [Online]. Available: https://tools.ietf.org/html/rfc5201#section-8

[15] R. Moskowitz, P. Nikander, T. Henderson, "Host Identity Protocol," IETF RFC 5201, April 2008.

[16] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," IETF RFC 2401, November 1998.

[17] OpenHIP. [Online]. Available: http://www.openhip.org

[18] "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," pp. 1 –2793, 2012.