Security of Wi-Fi On-board Intra-vehicular Communication: Field Trials of Tunnel Scenario

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

***Abstract*—Wireless communications are increasingly-often selected as a cable replacement for on-board vehicular networks. When a wireless technology implements safety critical application, cryptographic countermeasures are required. This paper describes the impact of security on intra-vehicular communication in a real tunnel scenario, e.g. for urban transit or mining vehicles where the usage of security is mandatory in order to maintain the system safety. The measurement campaign was carried out in a sport ski-tunnel using commercial off-the-shelf (COTS) Wi-Fi modules. The objective was to understand the impact of overhead on security in a tunnel considering line-of-sight (LOS) and non-LOS (NLOS) scenarios. In addition, the study compared different solutions for security to evaluating lesser known protocols. These field trials showed that wireless security is feasible up to 300 m in NLOS without repeaters. Finally, the experiment presented confirms the effectiveness of the Host Identity Protocol when used as standalone or in combination with other security solution.**

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

I. Introduction

The worldwide proliferation of wireless local area networks (WLAN) started many years ago and today Wi-Fi confirms its maturity. For a customer, one of the attractive advantages of WLAN technologies is cable replacement because it gives an immediate on the wireless investment. Wireless outdoor communications must operate in harsh conditions with multiple attenuated, delayed and phase-shifted echoes. This challenging multipath radio channel makes it harder to get usable WLANs. When Wi-Fi is selected for safety critical applications, e.g., urban transit and mining industries [1] new elements should be investigated. These systems require high safety levels which increase the complexity of design and test. First of all should be clear the difference between safety and security: safety avoids physical harm to humans and things whereas security applies defenses from malicious attacks [2]. Hacking a safety system in the best case could bring that to fail safe state, compromising the system availability [3]. In the worst case scenario fatal accidents occur to people. Europe has a dedicated standards body (i.e. CENELEC) to assure quality, safety and health of its citizens. For unified communications in rail systems, CENELEC [4] classifies Wi-Fi as open communication (i.e. category 3 in CENELEC 50159 [4]) requiring a cryptographic defense in order to resist to malicious attacks.

IEEE developed IEEE 802.11p and IEEE 1609.x grouping these standards in the wireless access in vehicular environments (WAVE) [5], [6]. The first standard is an amendment to IEEE 802.11 in order to include vehicular environments. IEEE 1609.x specifies additional layers needed in this specific application. WAVE includes vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) scenarios. IEEE 1609.2 implements security services in these architectures providing cryptographic mechanisms [6].

At the moment of this writing the authors didn't find any WAVE card ready for the integration inside a microprocessor board. Currently the market offers on-board units (OBUs) and road-side units (RSUs) that were closed standalone Linux platforms.

The objective of these field trials is to evaluate throughput loss due to security for intra-vehicular (i.e. inside the same vechicle) Wi-Fi based communication in a tunnel using COTS devices. The results achieved in the artificial ski-tunnel could be applied to similar scenarios, e.g., mining systems. Moreover, the solution proposed here could be easily implemented with commercial radios and software libraries.

The paper is organized as follows. In Section II the scenarios are investigated and in Section III the security layer tested. Section IV describes the measurements with the results presented in Section V.

II. Scenario

The scenario studied is an end-to-end connection (Figure 1) between two nodes, e.g., vehicles placed inside the tunnel. Each node is composed of Wi-Fi module, antennas and a controller (i.e. PC). The distance between the transmitter (TX) and the receiver (RX) is increased in order to simulate scenarios that we could have on-board with long vehicles in terms of LOS and NLOS. Head-to-tail communications for long vehicles shall consider NLOS scenario. With the first set of measurements, the scenario without any encryption was studied [7]. Subsequently the authors repeated measurements applying security protocols. IEEE standard 802.11-2012 [8] was used to implement the wireless on-board communication. In order to extend the maximum distance between TX and RX one repeater in the middle was introduced. The repeater insertion is suitable for long on-board link when

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

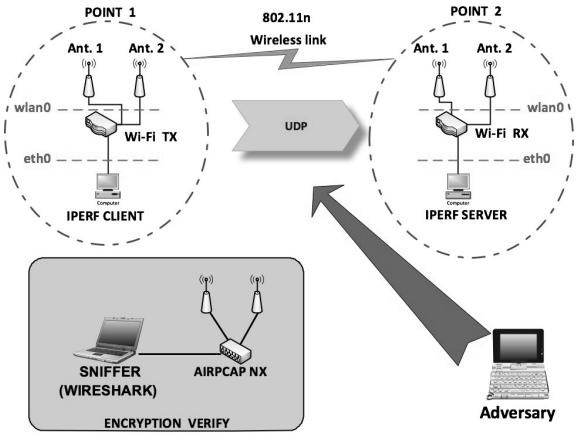

Fig. 1. Scenario: end-to-end communication and adversary position.

high availability of the wireless communication has to be guaranteed. In any case the network topology tested was a fixed infrastructure installed on-board the same vehicle. In this scenario the distance between the extremities of the wireless link is almost the same.

Finally, in this measurement campaign 2x2 MIMO technology was tested because it is a promising solution in intra-vehicular communication and scattering scenarios but the expected increment on performance is far away from the maximum theoretical capacity [9].

III. Security

Modern vehicles are controlled by complex distributed systems with a large number of processors, millions of lines of codes and physical interfaces [10]. For example an attacker embarked on the vehicle could launch intentional attack to the Wi-Fi on-board network tacking control of breaks, lighting, steering or entertainment subsystem.

Intra-vehicular on-board communications should consider the following attacks:

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

WLAN users are vulnerable to malicious attacks against standard encryption protocol, e.g., WPA (Wi-Fi Protected Access) was cracked several years ago [11], [12].

Standard Wi-Fi security protocol WPA2-PSK (Pre-Shared Key) was selected for the measurement campaign due to the WPA vulnerability. In addition, Host Identity Protocol (HIP) was tested because it offers end-to-end security and resistance to previous list of attacks [12]. The overhead due to security for intra-vehicular communication inside a tunnel is discussed in this paper describing briefly the protocols used.

The measurement campaign included three different security solutions implemented standalone or in combination part of those: WPA2-PSK, HIP and TOFINO. The combination of these protocols was tested in order to have a non-standard solution for security or *layered security*. Normally the attacker carries out a threat starting from the most commonly used protocols and having a combination of those could help only in terms of time needed to hack the communication.

WPA2-PSK: In 2001 Wi-Fi Alliance formed the IEEE 802.11i committee to increase MAC-layer security and in 2004 they included WPA2 in the standard [13]. In particular WPA2 replaced WPA and introduced the Counter mode with Cipher Block Chaining MAC Protocol (CCMP) [8]. CCMP protects the integrity of MAC Protocol Data Unit (MPDU) as shown in Figure 3, and provides services for data confidentiality and authentication [8]. During the measurement campaign, WPA2-PSK was adopted to implement a security protection at layer 2 of the OSI (Open Systems Interconnection) model. The shared secret used by each device to secure the traffic between the two points in the tunnel was a pass-phrase.

The *packet size overhead* introduced by WPA2-PSK is 16 B as shown in Figure 3.

HIP: Host Identity Protocol (HIP) is under continuous development in the IETF (Internet Engineering Task Force) and its specifications are in RFC5201 [14]. HIP allows the separation between the identification and localization information that normally comes with the IP-address. Moreover this protocol is designed against DoS and MitM attacks. HIP introduces the *host identity layer* in the TCP/IP stack between networking and transport layers. This protocol starts with the Base Exchange (BEX). BEX consists of a four-way handshake in order to establish a Security Association (SA) between the initiator and the responder. Each host has to generate its Host Identity Tag (HIT) used in BEX with one-way hash starting from a Public Key. After SA is established both hosts uses IP Security (IPSec) Encapsulating Security Payload (ESP). When pairing is completed HIP uses IPSec in order to exchange data via a secure tunnel (Figure 2). It implements a layer 3 tunneling solution. During the field trials in Vuokatti, an open source HIP implementation (i.e. OpenHIP [15]) was selected with IPSec ESP transport mode. Transport mode was used to protect end-to-end communication [16] encrypting only the IP payload (Figure 4). OpenHIP ran as a software library at user space level in a Linux laptop. This library created a new virtual network tap that was used to send/receive packets with Iperf tool [17].

The *overhead* added by OpenHIP includes a little less than 2

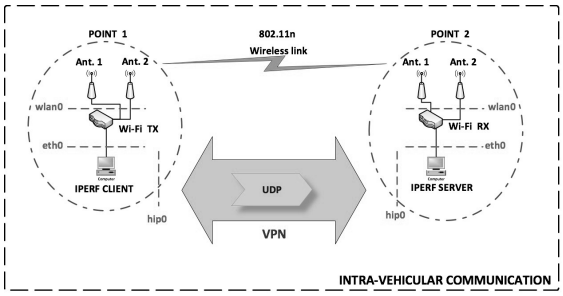

Fig. 2. Protected traffic

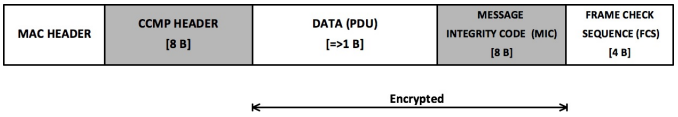

Fig. 3. MAC Protocol Data Unit (MPDU) when using CCMP

kB of exchanged data during BEX and a protocol packetization due to ESP security. The packetization consists of fixed-size fields (i.e. 8 B + 12 B) and ESP Tailer with variable length (i.e. 2 B + (min 0 B, max 255 B)).

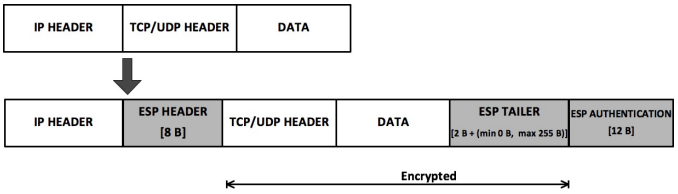

Fig. 4. IPSec: ESP transport mode

TOFINO: Tofino Endbox [18] was another implementation of HIP via external devices in accordance with Bump In The Wire (BITW) architecture. BITW uses a dedicated hardware device (i.e. Tofino Endboxes) to provide HIP service. Tofino started the HIP experience in the way to protect SCADA (Supervisory Control And Data Acquisition) devices where the closed network paradigm couldn't be applied anymore. Taking the advantage from this approach. Tofino Endboxes were used during tests where wireless network is open for its definition. These boxes installed between laptop and demonstrator devices (i.e. Wi-Fi TX and Wi-Fi RX in Figure 1) for each side built a virtual private network (VPN) between Wi-Fi TX and Wi-Fi RX creating a secure connection at layer 2 in the OSI model.

IV. Field Trials

The measurement campaign was carried out in a ski-tunnel located in Vuokatti (Finland) using a kit composed of Wi-Fi nodes. Each node consists of two antennas (i.e. supporting MIMO), one embedded PC with one Wi-Fi module compliant with IEEE 802.11 standard [8], cables (i.e. Ethernet, coaxial) and one adjustable heights stand. The tunnel's dimensions are shown in Figure 5. The length of the tunnel is 1.2 km with a maximum relief equal of 18 m as shown in Figure 6. The end-to-end communication presented in this experiment works similarly to an intra-vehicular (i.e. same vehicle) on-board network. The NLOS wireless on-board communication was evaluated because this scenario is similar to a mine tunnel or subway where there are several curves and it easier to have NLOS communication. On the other hand, real mining tunnels or subway scenarios have tunnel junctions whereas the ski-tunnel is only one pipe, which has an impact on signal propagation [19].

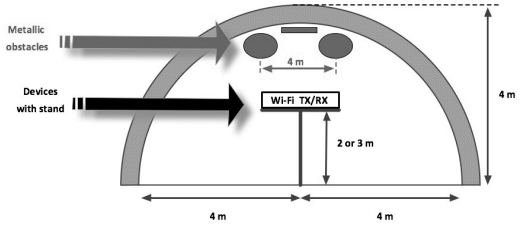

Fig. 5. Tunnel shape

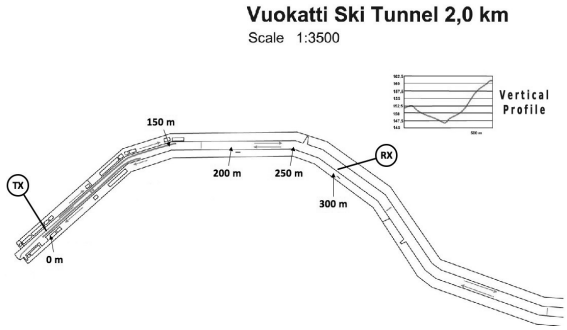

Fig. 6. Vuokatti Ski-tunnel map and TX/RX displacement

A. Setup

Figure 1 presents the measurements setup where each point or node was equipped with two antennas installed on a metallic plate. This plate was installed on a stand with an embedded Linux PC equipped with a Wi-Fi module compliant with IEEE 802.11 standard [8] and connected to the antennas. The embedded PC was driven by an external laptop used to run Iperf [17] server and client. The Iperf tool was needed for communication profiling that sent and received UDP traffic. When Tofino end-boxes were tested these were installed between the embedded Wi-Fi PC and a Windows laptop. The UDP buffer size was a default value, i.e., 160 kB (Linux) and 8 kB (Windows). Finally the setup included a sniffer composed by a laptop with installed AIRPCAP NX USB device [20] and Wireshark [21] software for protocol analysis. The sniffer was used only to verify the traffic encryption over the wireless link (Figure 1).

B. Measurements

The measurement campaign on security was carried out inside the tunnel following the scenarios reported in Section II. The first stand with the transmitter (i.e. Point 1 in Figure 1) was placed at the beginning of the tunnel and was not moved during the measurements. On the other side, the receiver changed its position, by being placed at the distances listed in Table I and the diagram presented in Figure 6. Starting from measurements without security described in [7], the communication was profiled again with Iperf but using a security protocol. Different configurations were evaluated considering both IEEE 802.11a+n and IEEE 802.11g+n protocol options provided by the Wi-Fi module, as well as both 5.8 GHz and 2.4 GHz frequencies bands. At the end the investigation on

TABLE I
WIRELESS LINK PARAMETERS

Parameter	Value
Radio protocol	802.11 g+n
Wi-Fi channel	9 (2452 MHz)
Transport protocol	UDP
Security protocols	WPA2-PSK, HIP
Transmitted power	20 dBm
Vital[1] bandwith	10 Mbps
Non-Vital[2] bandwith	54 Mbps
Antenna height	2 m
Distances	200, 150+150,[3] 250, 300 m
Link type	LOS, NLOS
Transmission duration	180 s

[1] Vital: Function implemented in fail-safe.
[2] Non-Vital: The function doesn't have safety implications.
[3] 150+150: 300 m end-to-end communication realized with 2 links and a repeater in the middle after 150 m.

security was concentrated on longer distances for NLOS (i.e. 200, 250 and 300 m) at 2.4 GHz because the solution at 5.8 GHz didn't achieve the desired bit-rate (i.e. at least 3 Mbps in NLOS). Moreover, a configuration with a repeater in the middle (i.e. 150 + 150 m) was tested to understand possible correlation between latency introduced by the repeater and throughput loss.

V. RESULTS

Throughput, jitter and packet loss were measured by using the same tool used for measurements without security (i.e. Iperf [17]). 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. On the other hand, during these tests over-the-air traffic wasn't recorded because AIRPCAP [20] with Wireshark [21] couldn't get any information about wireless signals reading encrypted packets.

The main goal in these tests was to understand which of the tested security protocols could have the best performances in terms of throughput loss for intra-vehicular communications in a tunnel. The parameters used were: range or distance (m), jitter (ms) and throughput (Mbps).

The strategy used to measure the security protocols overhead has already been presented in Section III (i.e. with Iperf). In particular Table II shows results achieved in terms of throughput for one IEEE 802.11g+n stream when these security protocols were used as standalone or combined together (i.e. layered security).

Figure 7 presents results using OpenHIP and OpenHIP in combination with WPA2-PSK at different distances. Each data point represent an average of 180 s transmission time. The measured mean throughput at 300 m with only OpenHIP was 5.83 Mbps. The mean jitter and packet lost increased due to the increment of the range and security doesn't have impact on these parameters.

A. Iperf results with security

To compare these measurements with similar scenarios without security defined in [7], the same Iperf configurations were used. When two data streams were applied, first and last 3 seconds of a measurement were discarded due to delay of manual start-up of two separate Iperf. Only the protocol IEEE 802.11g+n was tested with security because IEEE 802.11a+n couldn't achieved 150 m range.

The measurements were divided in two main groups, first without security [7] and afterwards with security. The wireless link goodness inside the tunnel was evaluated with the first set of tests. Basically the maximum range was identified without security and then tested by encrypting the wireless link in the way to evaluate the overhead introduced and the differences in performance. The measurements with security protocols were carried out only for links where the performances in terms of throughput were sufficient (Table II) and that choice was imposed by the time constraints. The performance analysis with security was based on lower number of measurements compared to without security. In any case those are sufficient to get a clear indication how to proceed. The results achieved indicate how the throughput is significantly affected by NLOS channel rather than security protocol overhead.

B. Throughput loss

Based on the results reported in the previous paragraph, Table II shows the overhead due to security comparing to tests with and without any encryption.

TABLE II
THROUGHPUT LOSS DUE TO SECURITY

Distance [m]	Security	Throughput [kbps]	Loss [%]
200[2]	No	9999	-
200[2]	OpenHIP	10000	0
$150 + 150$[3]	No	9999	-
$150 + 150$[3]	WPA2-PSK + OpenHIP	9910	0.9
250[1]	No	8906	-
250 [1]	WPA2-PSK	7883	11.5
250 [1]	TOFINO[4]	4544	48.9
250 [1]	WPA2-PSK + TOFINO[4]	4514	49.3
300 [2]	No	7865	-
300 [2]	OpenHIP	5833	24

[1] Omni-directional antenna
[2] Directional antenna
[3] Ends of communication used directional antenna and repeater omni-directional
[4] Measurements performed using Windows PC

The results with one data stream show that with WPA2-PSK, OpenHIP and combination of these, the maximum throughput loss achieved is 24% at 300 m (Table II). TOFINO end-boxes introduced a bigger reduction due to the devices'

performance and different buffer size on Windows compared with OpenHIP implemented in Linux laptop.

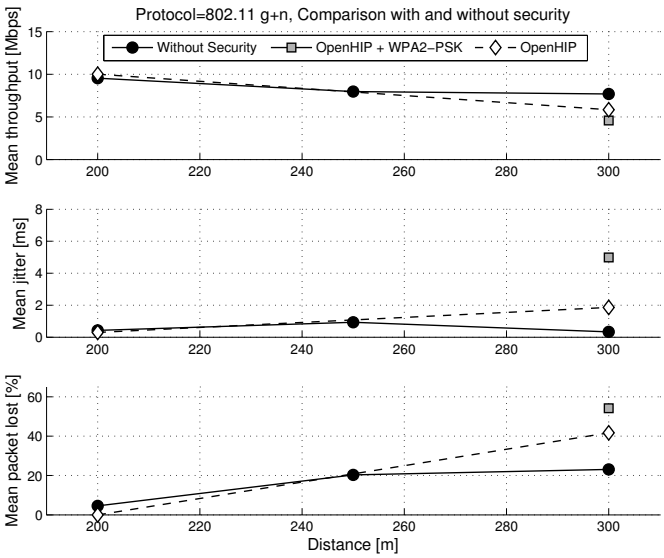

Fig. 7. Security comparison at different distances at NLOS scenario.

When measuring the throughput of two streams, the prioritization of these are not valid due to the encryption of the type-of-service (ToS) field. This information is encrypted and the MAC layer could not handle ToS with an erroneous prioritization. In order to have quality-of-service (QoS) requirement a different method has to be implemented.

VI. Conclusion and Future Works

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. Furthermore the security architecture tested would mitigate attacks to the wireless on-board network that could come from an attacker boarded on the same vehicle.

This experiment analyzed the NLOS scenario that could happen in head-to-tail on-board wireless communication for long vehicles.

Starting from the results achieved without security, more robust configurations were selected to test security performances.

The main conclusion (Table III) is that WPA2-PSK, OpenHIP and its combination introduce an acceptable overhead in terms of throughput loss, jitter and packet loss up to 300 m without any repeater and in NLOS configurations. The acceptance criteria required at least 3 Mbps of real throughput above 200 m in NLOS. A communication with two independent and concurrent streams set up manually confirmed the trend achieved without security where the communication were unbalanced. One reason is the manual launching of Iperf instances: the service that has been started first has the better performances combined to the erroneous interpretation of ToS field. Extending the range over 300 m the performance declines sharply leaving this distance as the maximum achievable.

TOFINO end-boxes needed Windows PC and it implied a different buffer size: OpenHIP used 160 kB and TOFINO only 8 kB. In addition, the security protocol applies computation resources of TOFINO devices which are limited compared to OpenHIP running in a laptop. TOFINO end-boxes had worst performance due to the measurement layout that was different than with OpenHIP. On the other hand BITW architecture is interesting and useful because it maintains separate security technology from the radios selected.

Security is one of the important issues in vehicular communications and in the future could be interesting compare IEEE 1609.2 with HIP-based solution.

TABLE III
Main Results on Security

N	Result	Conclusions
1	*WPA2-PSK + OpenHIP* had an acceptable throughput loss.	*WPA2-PSK* had a good maturity and *OpenHIP* introduced an interesting diversity in the security protocols.
2	*TOFINO* end-boxes did not get enough guarantees to continue in its utilization.	*TOFINO* end-boxes performance was not so good and this hardware needs a customization for industrial application.
3	The introduction of security is feasible till 300 m in NLOS.	The throughput loss with security protocols did not compromise the end-to-end communication and guarantees good performances in terms of throughput.

VII. Acknowledgment

Authors would like to thank Mario Papini for drawing our attention to security and moreover to Madhusanka Liyanage, Pradeep Kumar and Jani Pellikka for their technical support.

References

[1] P. Misra, S. Kanhere, D. Ostry, and S. Jha, "Safety assurance and rescue communication systems in high-stress environments: A mining case study," *Communications Magazine, IEEE*, vol. 48, no. 4, pp. 66 –73, 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] K. Hansen, "Security attack analysis of safety systems," *Emerging Technologies Factory Automation, 2009. ETFA 2009. IEEE Conference on*, pp. 1–4, 2009.

[4] "CENELEC EN 50159 - Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems," 2012.

[5] R. Uzcategui and G. Acosta-Marum, "Wave: A tutorial," *Communications Magazine, IEEE*, vol. 47, no. 5, pp. 126 –133, May 2009.

[6] K.-Y. Ho, P.-C. Kang, C.-H. Hsu, and C.-H. Lin, "Implementation of WAVE/DSRC Devices for vehicular communications," vol. 2, pp. 522 –525, May 2010.

[7] H. Viittala, S. Soderi, J. Saloranta, M. Hämäläinen, and J. Iinatti, "An Experimental Evaluation of WiFi-Based Vehicle- to-Vehicle (V2V) Communication in a Tunnel." Vehicular Technology Conference (VTC2013-Spring), June 2013.
[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," pp. 1 –2793, 2012.
[9] J. A. Valdesueiro, B. Izquierdo, and J. Romeu, "MIMO channel measurement campaign in subway tunnels," in *Antennas and Propagation (EuCAP), 2010 Proceedings of the Fourth European Conference on*, April 2010, pp. 1 –4.
[10] Comprehensive Experimental Analyses of Automotive Attack Surfaces . [Online]. Available: http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[11] Researchers Crack WPA Wi-Fi Encryption. [Online]. Available: http://it.slashdot.org/story/08/11/06/1546245/researchers-crack-wpa-wi-fi-encryption
[12] 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.
[13] "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 Amendment 6: Medium Access Control (MAC) Security Enhancements," pp. 01 –175, 2004.
[14] HIP. [Online]. Available: http://datatracker.ietf.org/wg/hip/charter/
[15] OpenHIP. [Online]. Available: http://www.openhip.org
[16] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley and Sons, 2008.
[17] Iperf. [Online]. Available: http://iperf.fr
[18] Tofino. [Online]. Available: http://www.tofinosecurity.com
[19] M. Hamalainen, J. Talvitie, V. Hovinen, and P. Leppanen, "Wideband radio channel measurement in a mine," in *Spread Spectrum Techniques and Applications, 1998. Proceedings., 1998 IEEE 5th International Symposium on*, vol. 2, sep 1998, pp. 522 –526 vol.2.
[20] AIRPCAP. [Online]. Available: http://www.riverbed.com/us/products/cascade/wireshark_enhancements/airpcap.php
[21] Wireshark. [Online]. Available: http://www.wireshark.org