High-mobility effects on WLAN fast re-authentication efficiency

Mohamed Kassab
IT/TELECOM-Bretagne/RSM
2, Rue de la chataigneraie
Cesson Sevignes, France
mkassab@telecom-bretagne.eu

Safaa Hachana
IT/TELECOM-Bretagne/RSM
2, Rue de la chataigneraie
Cesson Sevigne, France
shachana@telecom-bretagne.eu

Jean Marie Bonnin
IT/TELECOM-Bretagne/RSM
2, Rue de la chataigneraie
Cesson Sevigne, France
jm.bonnin@telecom-bretagne.eu

Abdelfettah Belghith
ENSI/CRISTAL LAB/HANA
Research Unit
Manouba Campus, Tunisia
abdelfattah.belghith@ensi.rnu.tn

ABSTRACT

Different fast re-authentication methods have been proposed to reduce the secure handover latency in 802.11 networks. Fast re-authentication methods perform proactive distribution of authentication keys avoiding authentication exchanges during network re-entry. The efficiency of these methods depends on their ability to propose proactive mechanisms that supports high velocities. In this paper, a comparison of the station velocity influence on the proactive distribution performance is given for several re-authentication methods. Three methods have been evaluated under a simulation environment.

Keywords

IEEE 802.11, fast handover, Pre-authentication, vehicular networks

1. INTRODUCTION

Next generation networks i.e. 4G networks, are foreseen as the integration of different existing wireless technologies. The result has to be a network ensuring seamless handovers from one technology to another while providing a continuous service to mobile users. WLAN wireless networks, such as IEEE 802.11, have been designed to offer wireless connectivity with a moderate mobility. To be efficiently integrated, in the same global network, with classic cellular networks e.g. GPRS, UMTS, CDMA 2000, etc. WLANs must ensure a better mobility support.

In 802.11 networks, a handover occurs when a mobile station moves out from the radio coverage area of its actual serving Access Point (AP) to a new one (a target AP). This handover can be classified to intra and inter-subnet handover based on positions of serving and target APs in the IP infrastructure. The intra-subnet handover occurs when concerned APs are under the same IP subnet. It only requires the reestablishment of link layer connectivity. Operations required by this re-establishment are named layer-2 handover and they consist in negotiation of layer-2 parameters. The inter-subnet handover occurs when involved APs are under different IP subnets. In this case, a layer-2 handover is followed by a layer-3 handover. The layer-3 handover is related to the maintenance of the network-layer connectivity and the rerouting of data flow to the new location.

In the initial versions of IEEE 802.11, the mobility performances of the protocol were mostly deteriorated by the layer-3 handover procedure. This was due to the simplicity of layer-2 handover where interactions were essentially performed between the mobile station and the AP. However, the link layer in IEEE 802.11 has evolved by integrating additional functionalities related to QoS, Security, etc. These functionalities add management exchanges to the layer-2 handover requiring interaction with entities in the core network and so increase handover latency. Particularly, the establishment of security mechanisms specified by the IEEE 802.11i extension induces a latency time up to 1 second during the network entry. Therefore, the layer-2 handover optimization remains an essential condition to offer seamless handover in both intra and inter sub-network mobility. In our previous works, we were interested in ensuring seamless mobility over secure IEEE 802.11 networks. We proposed two fast re-authentication methods: *Proactive Key Distribution (PKD) with anticipated 4-way-handshake* and *PKD with IAPP caching*. We have reduced strongly the duration of the authentication exchange between the station and the network. Thus, we have ensured low handover latency [2]. We evaluated the re-authentication time achieved by these methods, and found a latency less than 50 ms. The latter value ensures the support of service continuity even for sensitive real-time application e.g. VoIP.

QShine 2008, July 28-31, 2008, Hong Kong, Hong Kong.
Copyright 2008 ICST ISBN 978-963-9799-26-4
DOI 10.4108/ICST.QSHINE2008.4184

Otherwise, when WLANs will coexist with classic cellular networks, they must support communication continuity over high-mobility environments. In fact, there is a need to propose management mechanisms able to ensure handover preparation for stations moving with high velocity. In the particular case of authentication, the management mechanisms have to be able to perform key pre-distribution with neighbor APs before the actual execution of a handover. We propose to evaluate the effect of station velocity on the efficiency of the proactive distribution proposed by our fast re-authentication methods. For these purposes, we perform evaluation tests over a discrete event simulator named SimulX [6].

This paper is structured as follows. Section 2 presents work related to the high-velocity effect on WLAN performances. Section 3 describes the two solutions that we have proposed for a fast re-authentication in IEEE 802.11 networks. Section 4 presents the conducted simulation tests and obtained results. Finally, in section 5, we propose some concluding remarks.

2. RELATED WORK

High-velocity support was not one of the main goals when IEEE 802.11 protocol has been specified. As a consequence, handover performances may vary when station velocity exceed a certain threshold. Several works studied the performances of 802.11 WLANs in a high-speed environment. These works can be classified into two categories according to the proprieties they evaluated.

The first category focused on the effects of station velocity on wireless link performances and does not treat handover purposes. For example, [8] discusses possibilities and limitations of the use of 802.11 technology to connect fast moving vehicles. Evaluation tests measure data transmission performances of terminal moving in the range of a single access point. Authors have evaluated how varying the distance between a terminal and its AP can affect the exchanged traffic. In similar work, [9] proposes a performance evaluation of 802.11 link in different vehicular traffic and mobility scenarios. The Authors have concluded that 802.11 equipments are suitable for inter-vehicular communications; however, the 802.11 link performance (throughput, number of lost packets, SNR, etc.) is observed to degrade in increasingly hostile communication scenario such as large distance between peers or high velocity. In fact, the link quality or the Signal Noise Rate (SNR) is observed to degrade with increasing velocity or distance between peers. Additionally, Throughput shows a decreasing trend with increasing distance and velocity.

The second category studied the influence of station movement speed on the signaling load produced by mobility management protocols [7, 1]. In [7], authors have performed simulation to evaluate performances of layer-3 mobility management protocol, i.e. Mobile IPv6, Hierarchical MIPv6, etc. depending on mobile velocity. In [1] the authors have proposed a new solution to manage handover in WLAN networks based on a Handoff Anchor Point acting as a facilitator for handover decision and execution. The performances of the solution are evaluated through simulation studies. Particularly, the signaling cost is evaluated depending on high-speed environment and a curve presenting the signaling load against of the handover rate per minute is proposed.

As shown, many researchers studied the performances of WLANs in high mobility environments. Nevertheless, the ability of mobility management mechanisms to ensure acceptable handover latency reduction even in high-velocity environment is still an open issue. An additional point to be studied is the ability of management mechanisms to perform an efficient handover preparation for a fast moving station.

3. IEEE 802.11 FAST RE-AUTHENTICATION METHODS

IEEE designed a security architecture for IEEE 802.11 network presented in the IEEE 802.11i extension [4]. IEEE 802.11i propose a security skeleton based on three entities: the Supplicant, the Authenticator and the Authentication Server. The Authenticator (Access Point) relays authentication packets between the Authentication Server (AAA server) and the Supplicant (Mobile Station), while preventing other packets to pass through it.

IEEE 802.11i establishes a mutual authentication between stations and network and generate cryptographic suite to secure data exchanges. It defines an authentication key hierarchy and key generation exchanges. Figure 1 shows the 802.11i authentication exchange using one of the supported authentication methods, namely EAP/TLS.

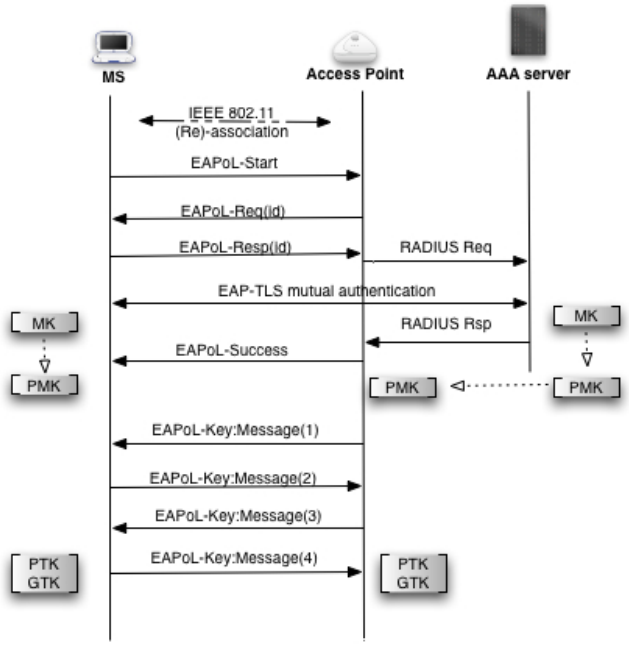

Figure 1: IEEE 802.11i authentication exchange

Firstly, the mutual authentication exchange between the MS and the AAA server allow them to generate separately a key named Master Key (MK). Secondly, a second key is derived from the latter: Pairwise Master Key (PMK). AAA server sends this new key to the access point. Finally, the MS and the AP prove the possession of the same PMK, through

an exchange of EAPoL-Key messages: the 4-way-handshake exchange. It results in a suite of cryptographic keys: the Pairwise Transit Key (PTK).

A second class of keys, *Group Transient Key(GTK)*, is also defined for the broadcast traffic. Every AP generates periodically a fresh GTK that it sends to associated stations using the Group-Key-Handshake exchange. The latter exchange consists of two EAPoL-Key messages. During an authentication exchange, the GTK is sent to station using the 4-way-handshake in conjunction with the generation of the PTK.

IEEE 802.11i has not been designed to support fast handover; an authentication can last up to 1s [5]. Several works have been proposed to provide fast and secure handover over IEEE 802.11 networks [2]. One of the most interesting propositions is the Proactive Key Distribution (PKD) [5]. We have re-evaluated through actual experimentation the handover time achieved by the PKD method and found that latency has leveraged to no less than 200 ms under realistic network load [2]. Such latency is rather too large to support real time applications. We proposed two fast re-authentication mechanisms based on the PKD method and showed that they yield to much better handover performances [2]. In the following section, we propose a description of these methods.

3.1 Proactive key distribution (PKD) method

The PKD method defines a fast re-authentication method following the authentication scheme amended by the IEEE 802.11i. It establishes authentication keys in potential target APs before the station re-association based on a proactive distribution. The key pre-distribution is based on a data structure named Neighbor Graph. This graph captures dynamically the ever-changing topology of the network and tracks the set of neighbor APs with which mobile stations may handover in the near future. The Neighbor Graph is managed by a centralized entity i.e. the AAA server.

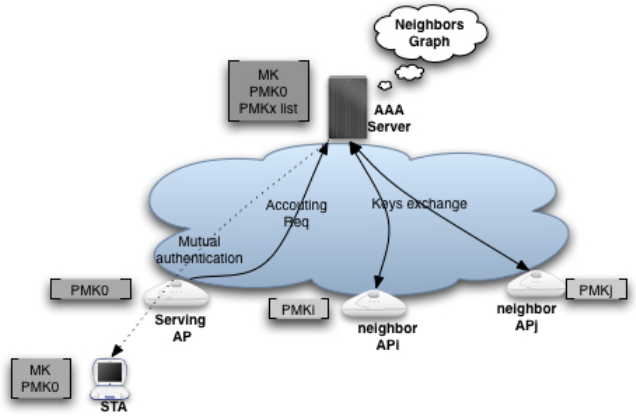

Figure 2: PKD pre-authentication exchange

Figure 2 shows exchanges specified by the PKD method to pre-distribute authentication keys. Firstly, an AP informs the AAA Server about a station authentication using an Accounting-Request. Secondly, the AAA Server performs a key exchange with each AP in the neighborhood of the serving AP to perform the keys pre-distribution. Finally, the AAA server generates specific PMK keys for each neighbor AP accepting pre-authentication and distributes them through Access-Accept messages. The PMK keys are generated through a recursive equation that use last generated PMK, AP identity and station identity [5].

At the time of handover, authentication exchange between the mobile station and the target AP is reduced to the 4-way-handshake since other necessary information has already been set up in the AP.

In previous work, we have demonstrated over test-bed experimentations that the more exchanges are performed during the handover execution, the more the HO latency will be variable. In fact, exchanges are sensitive to the transmission delay and the layer-2 retransmission frequency that depends on the wireless cell load and the signal quality [2]. As a result, the time needed to perform re-authentication during a handover depends extremely on the wireless network conditions. Thus, there is a need to reduce these exchanges to ensure an acceptable handover latency even under high loaded network [2].

3.2 PKD with IAPP caching method

The *PKD with IAPP caching* fast re-authentication method is based on the proactive key distribution defined in the PKD method [2] . This pre-distribution is associated to an additional key distribution between neighbor APs performed using the Inter Access Point Protocol (IAPP) [3].

The IAPP is an extension to the IEEE 802.11 standard defined by the TGf task group. This protocol proposes a transfer of network entry parameters related to a mobile station, during handover between a neighbor AP and the serving AP. Optionally, it defines a caching mechanism that enables transferring station contexts even before handover execution.

The *PKD with IAPP caching* uses the IAPP context transfer to perform a pre-distribution of PTK keys in addition to PMK pre-distribution performed by the PKD method. Pre-distributed PTKs are computed by the serving AP and sent to neighbors APs [2]. A PTK allows a mobile station to be authenticated temporarily with a target AP through a group-key-handshake [2]. Indeed, the station shall start a legacy PKD authentication with its new serving AP while continuing its data transmission.

As shown in Figure 3, a serving AP informs the AAA server about a new association in order to start PMK generation used to complete the proactive authentication procedure. Then, the serving AP consults its Neighbor Graph and starts an IAPP exchange to update neighbor AP caches. When the station moves to a target AP, it starts group-key-handshake using the cached PTK after which it will be able to re-start communications. During the data transmission, a 4-way-handshake is started in order to compute a new PTK.

3.3 PKD With Anticipated 4-way-handshake

The *PKD With Anticipated 4-way-handshake* method is also based on the PMK pre-distribution defined in the PKD

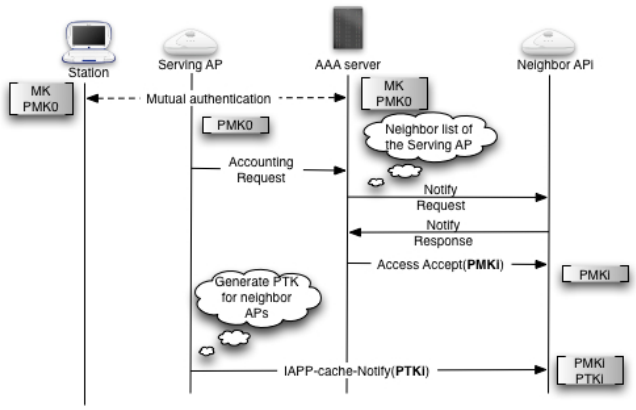

Figure 3: PKD with IAPP caching exchange

method[2]. In addition to the PKD pre-distribution, 4-way-handshake exchanges between a station and neighbor APs are anticipated through the wireless connection established with the current serving AP[2].

The pre-authentication mechanism is trigged by a station association or re-association. Firstly, the new serving AP informs the AAA server that starts a proactive key distribution. As a result, all neighbor APs receive PMK keys related to the station. Secondly, the station and neighbor APs carry out a pre-authentication through the core network. Each neighbor AP executes a 4-way-handshake with the station through the serving AP using the PMK key pre-distributed by the AAA server. These exchanges are shown in Figure 4.

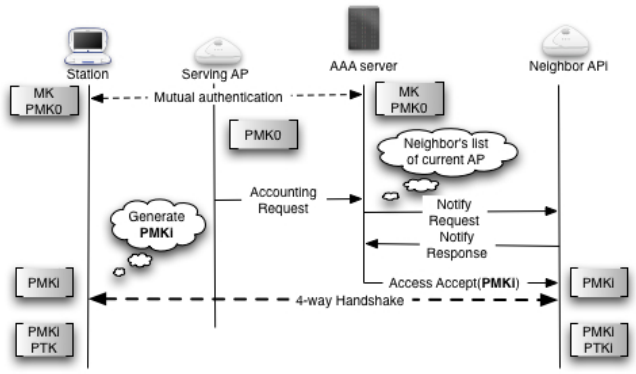

Figure 4: PKD with anticipated 4-way-handshake exchange

When the station moves toward a neighbor AP, it has already computed the PTK key through the anticipated 4-way-handshake. Therefore, it only carries out a group-key-handshake with the target AP to complete the authentication.

4. SIMULATION SCENARIOS AND RESULTS

To evaluate fast re-authentication methods, we have integrated them in a simulation environment. The advantage of a performance evaluation, based on simulation tests, is the ability to perform test scenarios that are not easy to deploy in testbeds or real environments. We choose an event-driven simulator named SimulX [6]. This simulator is an open source project developed under the collaboration of several universities and research labs. SimulX was designed to experiment mobility management protocols in an IPv6 world.

As we are interested by evaluating the performance of re-authentication methods under a high mobility environment, we consider a 802.11 wireless access in a highway. Vehicles, which travel on the highway, benefit from wireless connectivity through Access points deployed in the roadside. APs are connected to a AAA server through a backbone network. Figure5 shows the considered network deployment.

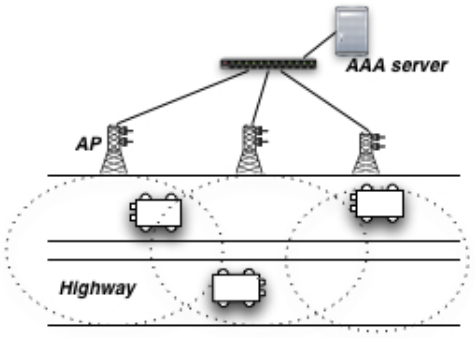

Figure 5: AP deployment in the highway roadside

In a fisrt scenario, we consider a mobile station moving through the radio coverage of 30 APs placed linearly on the station trajectory. The transmission range of an AP is at most 100 meters and distance between two neighbor APs is 160 meters. APs are inter-connected using an Ethernet based core network. The mobile station has an ongoing traffic with a correspondent node located in the core network. We measure the re-authentication time when station moves through the wireless network. We vary the station velocity and plot the variation of authentication time depending on this parameter as shown in Figure 6.

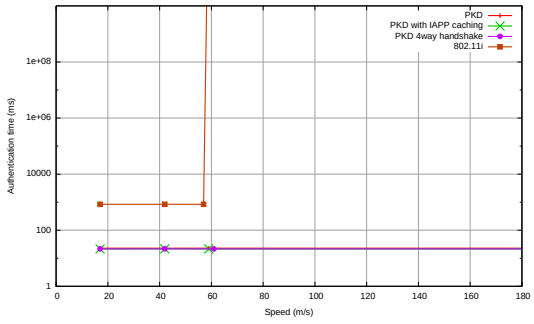

Figure 6: Velocity effect on the authentication time

The basic IEEE 802.11i authentication offers a regular authentication time until the station velocity reaches 57 m/s.

Exceeding the latter value, the station is no longer able to perform the authentication with the AAA server. In fact, the crossing time of a cell is too short to the execution of a full authentication. With fast re-authentication methods, the station performs re-authentications with a regular time with velocities higher that 180 m/s.

It is clear that key pre-distribution, proposed by fast re-authentication methods, presents a real improvement regarding the standard IEEE 802.11i authentication. In addition to the reduction of latency induced to traffic, these methods enhance the reliability of authentication process in high-speed environment.

Noticing the fast re-authentication method performances in the previous scenario, we propose to perform additional tests to show the limits of these mechanisms. We propose to evaluate fast re-authentication method performances in extreme conditions. We reduce APs coverage to 30 meters and the distance between two neighbor APs to 50 meters. The station moves in a linear trajectory with a distance of 13 meters from APs. Figure7 shows the variation of the HO latency related to this scenario.

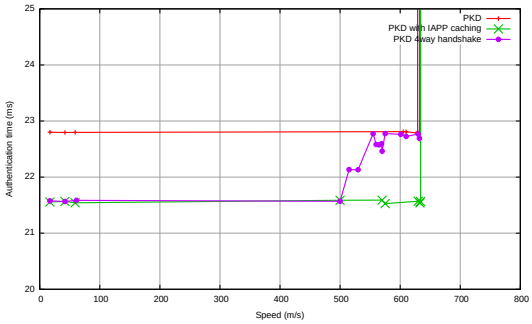

Figure 7: Fast re-authentication methods limits

The *PKD* method offers a constant authentication time with velocities up to 630 m/s. Beyond this limit, the centralized key pre-distribution is not performed before the station starts HO execution with neighbor AP.

For the *PKD with anticipated 4-way-handshake*, we can spot three parts. For velocities lower than 500 m/s, the re-authentication method ensures a constant re-authentication time corresponding to the usual method performance. For velocities from 500 to 575 m/s, we notice an irregular growth of the authentication time average. This is due to the failure of the pre-negotiation mechanism defined by this method in some HO preparations executed by the station that results on re-authentications based on the PKD preparation. In these cases, the average of the HO latency increases with the increase of the number of unsuccessful pre-negotiations. For velocities up to 575 m/s, the station is not able to perform keys pre-negotiation with neighbor APs and so the re-authentication is fully based on the PKD preparation. As a result, *PKD with anticipated 4-way-handshake* have the same performances as the *PKD* method.

PKD with IAPP caching offers a constant authentication time performances equal to the usual method performance until the velocity limit imposed by the PKD pre-distribution.

It is interesting to notice the difference between *PKD with anticipated 4-way-handshake* and *PKD with IAPP caching* performances. In fact, the context transfer proposed by *PKD with IAPP caching* is more adapted to the high speeds since it enables the regularity of the authentication time until the limit imposed by the centralized proactive distribution(i.e. the PKD key distribution). This is not the same with the pre-negotiation mechanism proposed by *PKD with anticipated 4-way-handshake*. The latter method has also the drawback to generate more burdens on the wireless link.

Based on previous observations, it is clear that performances of all studied fast re-authentication methods are limited by the centralized proactive distribution defined by the *PKD* method. The time needed to perform the preparation have to be shorter than the cell crossing time to result into a successful re-authentication in the next cell.

More generally, the velocity limit supported by proactive HO preparation mechanisms depends on the delay imposed by parameter establishment performed on the preparation phase. The previous delay is mainly due to exchanges with centralized entities (i.e. the AAA server). Therefore, the amount of exchanges, performed with centralized entities, defines the velocity limit of a HO preparation mechanism.

Additionally, we can conclude that anticipated parameter negotiation performed between the mobile station and the network may reduce the performance of HO preparation mechanisms. In fact, this mechanism increases the preparation phase duration and so may result in a reduction of the preparation efficiency within high velocities.

5. CONCLUSION

In this paper, we have been interested to the ability of secure IEEE 802.11 network to support communication continuity in high-mobility environments. We have proposed to evaluate the efficiency of the authentication procedure in high mobility environment.

In a previous work, two fast re-authentication methods ensuring low handover latency in IEEE 802.11 networks have been proposed. We evaluate the effect of station velocity on the efficiency of proposed fast re-authentication methods and compare the results with performances of the basic IEEE 802.11i authentication and the well-known PKD re-authentication method. This evaluation is based on tests performed on a simulation environment.

Results show that basic IEEE 802.11i authentication is not adapted to high mobility environment. On the other hand, a mobile station performs authentications with a regular time with velocities up to 500 m/s with *PKD*, *PKD with IAPP caching* and *PKD with anticipated 4-way-handshake*. Additionally, we notice that studied fast re-authentication methods have a limitation in velocity support. This limit is due to the centralized proactive distribution defined by the *PKD* method. Nevertheless, *PKD with IAPP caching* ensure a better support of high velocity while guarantying a HO latency regularity.

Based on obtained results, we propose some general conclusions related to HO preparation expected behaviors in high

mobility environment. Exchange performed with centralized entities limits the velocity supported by a HO preparation mechanism. In addition, context transfer offers better performances than anticipated parameter negotiation in high mobility environments.

In future work, we aim to evaluate the effects of additional network conditions, such as: core network architecture and wireless network load, into the performances of handover preparation mechanisms

6. REFERENCES

[1] S. Ahmad, M. Akbar, and M. Qadir. High Speed Scalable Mobility Management Architecture over Infrastructural WLAN. *Multitopic Conference, 2006. INMIC'06. IEEE*, pages 343–348, 2006.

[2] M. Kassab, A. Belghith, J. Bonnin, and S. Sassi. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. *1st ACM workshop on Wireless multimedia networking and performance modeling*, pages 46–53, 2005.

[3] LAN/MAN Standards Committee. IEEE 802.11f: IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. Standard, IEEE Computer Society, July 2003.

[4] LAN/MAN Standards Committee. IEEE 802.11i: Amendment 6: Medium Access Control (MAC) Security Enhancements. Standard, IEEE Computer Society, April 2004.

[5] A. Mishra, M. ho Shin, and W. A. Arbaugh. Pro-active key distribution using neighbor graphs. *IEEE Wireless Communications*, 11, 2004.

[6] N. Montavont, J. Montavont, and S. Hachana. Wireless IPv6 simulator: SimulX. *40th Annual Simulation Symposium, Norfolk, VA, Part of the 2007 Spring Simulation Multiconference*, March 2007.

[7] L. Osborne, A. Abdel-Hamid, and R. Ramadugu. A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, and Mobile IPv6 Regional Registrations. *Wireless Networks, Communications and Mobile Computing, 2005 International Conference on*, 2, 2005.

[8] J. Ott and D. Kutscher. Drive-thru Internet: IEEE 802.11 b for "automobile" users. *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, 1, 2004.

[9] J. Singh, N. Bambos, B. Srinivasan, and D. Clawin. Wireless LAN performance under varied stress conditions in vehicular traffic scenarios. *Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th*, 2, 2002.