Secure Handoffs for V2I Communications in 802.11 Networks

Carlos H. Gañán
Departament d'Enginyeria Telemàtica
Univ. Politècnica de Catalunya
Barcelona, Spain.
carlos.ganan@entel.upc.edu

Sergi Reñé
Departament d'Enginyeria Telemàtica
Univ. Politècnica de Catalunya
Barcelona, Spain.
sergi.rene@entel.upc.edu

Jose Muñoz-Tapia
Departament d'Enginyeria Telemàtica
Univ. Politècnica de Catalunya
Barcelona, Spain.
jlmunoz@entel.upc.edu

Oscar Esparza
Departament d'Enginyeria Telemàtica
Univ. Politècnica de Catalunya
Barcelona, Spain.
oesparza@entel.upc.edu

Jorge Mata-Díaz
Departament d'Enginyeria Telemàtica
Univ. Politècnica de Catalunya
Barcelona, Spain.
jmata@entel.upc.edu

Juanjo Alins
Departament d'Enginyeria Telemàtica
Univ. Politècnica de Catalunya
Barcelona, Spain.
juanjo@entel.upc.edu

ABSTRACT

Vehicular ad hoc networks (VANETs) are emerging as a novel paradigm for safety services, supporting real-time applications (e.g., video-streaming, Internet browsing, online gaming, etc.). However, maintaining ubiquitous connectivity remains a challenge due to both high vehicle speed, and non-homogeneous nature of the network access infrastructure. Getting access to the network infrastructure must be controlled and only authorized users should be able to use it. However, the authentication process incurs in a not-negligible delay which can result in packet losses and other issues during handoffs. Hence, a fast and secure handoff scheme is essential. Although some solutions have been given in IEEE 802.11i and 802.11r standards, the handoff latency is still above 50 ms. Other protocols such as CAPWAP and HOKEY include support for fast handoff but have not been evaluated in a vehicular network. In this article, we analyze the security properties and performance of current proposals. Finally, simulations are conducted to date the effectiveness of the handoffs schemes.

Categories and Subject Descriptors

C.2 [**COMPUTER-COMMUNICATION NETWORKS**]: Security and protection; K.6.5 [**Security and Protection**]: Authentication

Keywords

handoffs, security, vehicular-to-infrastructure

PE-WASUN'13, November 3–8, 2013, Barcelona, Spain.
Copyright 2013 ACM 978-1-4503-2361-1/13/11
http://dx.doi.org/10.1145/2507248.2507274 ...$15.00.

1. INTRODUCTION

Road and vehicle circulation systems, which are one of the most important infrastructures and are supporting the humans' daily life, have Internet communication necessities. Intelligent Transportation Systems (ITS) aim to optimize the social costs of road systems and enhance their security as well as drivers comfort by allowing such services as fleet management, navigation, billing, multimedia applications, etc. by using vehicular networks. To achieve fully mobile communications in vehicular networks, handoff procedures can perform data flow migrations from a correspondent node (e.g., an Internet server placed in the wired network) and vehicles equipped with On-board units (OBUs) between different points of attachment named Road Side Units (RSU), using Vehicle-to-Infrastructure (V2I) communications.

In spite of the numerous advantages by launching VANETs, security issues have to be well addressed before putting these application scenarios into practice. AAA (Authentication, Authorization and Accounting) infrastructures have been proposed to provide access control. Integrated with AAA infrastructures, the Extensible Authentication Protocol (EAP) [7] provides flexible authentication and key management for network access control. However, authenticating an OBU moving from one RSU to another raises a challenge. Different from network handoff, the research purpose of security handoff optimization is to reduce the latency of authentication and security key agreement when handoff from one RSU's coverage region to another. In traditional wireless LAN, handoffs have already been analyzed [2, 4, 13, 17, 19].

The IEEE 802.11f [2] standard specifies the fundamental architecture of communications between RSUs in order to support vehicle roaming from one RSU to another during the handoff period. However, due to the use of a RADIUS [15] server to manage RSUs, the handoff period is too long to support the real-time applications such as video streaming or voice over IP. To reduce this delay and provide security during the handoff, the 802.11i [3] and the 802.11r [4] protocols were proposed. The 802.11i was envisioned to deal with existing security inadequacies of the previous protocol. This protocol is based on separating the authentication from the message protection process allowing for embedding many currently stationary-approved authentication protocols like Kerberos and EAP with Transport Layer Security (TLS) [9] into the wireless networking domain. The main drawback of this standard is the considerable amount of time that it takes to authenticate, which makes it difficult to support real-time networking applications. Thus, to decrease the handoff latency the IEEE 802.11r was proposed [4]. This standard specifies fast Basic Service Set (BSS) transitions between RSUs by redefining the security key negotiation protocol. Consequently, the mobile device is entirely in charge of deciding when to handoff and to which RSU it wishes to handoff which allows both negotiation and requests for wireless resources.

These standards trigger the handoff procedure according to the power of the signal received from the current service providing RSU. However, using this method to detect the signal and locate a target RSU is time-consuming. Even when using a Geographical Positioning System (GPS) to predict the best RSU [16], this procedure accounts for more than 80% of the overall handoff delay [18]. Moreover, the standard IEEE 802.11r does not support the inter-domain handoff. To support roaming between different operator, the Internet Engineering Task (IETF) proposed HandOver KEY (HOKEY) [14] protocol that enhances the EAP protocol to achieve low latency handoffs and method-independent fast re-authentication. The IETF also proposed the Control and Provision of Wireless Access Points (CAPWAP) [10] protocol to centrally manage access points and provide compatibility between multiple vendors in a large-scale environment, allowing mobile users to roam freely.

In summary, each of these protocols offers different capabilities to deal with the problem of secure fast handoff. In this paper we briefly describe each protocol emphasizing their security properties. We analyzed the delay they incur when moving from one RSU to another, and perform and in-depth evaluation in a vehicular scenario. Finally, we conclude the article.

2. HANDOFF IN VEHICULAR NETWORKS

Handoff in the IEEE 802.11 is the process for a mobile node (MN) to change its association with the APs when the received signal strength drops below a certain threshold value. In vehicular networks, the AP is an RSU while the MN is a vehicle that could be potentially moving at high speeds. The vehicle starts a scanning process to find another AP by switching to all available channels to transmit probe messages and/or receive beacons from the RSUs. Once a good candidate AP is found, an authentication and re-association phase is started involving the transfer of credentials from the old RSU to the new RSU. When the vehicle becomes successfully associated to the new AP and establishes communication, the handoff process is considered complete. Figure 1 shows the overall exchange of frames during the handoff process and the respective delays. Nevertheless, the IEEE 802.11p standard [5] defined for vehicular networks presents some particular differences when performing the handoff. IEEE 802.11p defines layer 1 and layer 2 adaptations to the 802.11 WLAN standard but lacks from management frames and no beacons are sent by the APs which complicates the handoff process. This standard aims to achieve fast adaptation to the rapid changes occurring in vehicular networks, sacrificing authentication procedures.

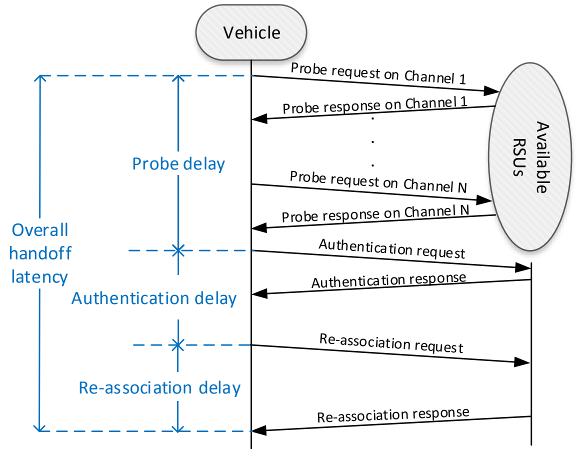

Figure 1: Delays during traditional 802.11 handoff in a vehicular network

IEEE 802.11p specifies a minimized set of parameters (i.e. WAVE Basic Service Set (WBSS)) for handoff process in order to make it more efficient the data exchange between vehicles and RSUs. The WBSS is announced through the WAVE Service Announcement (WSA), i.e., a beacon from the RSU in the case of V2I communication. Any vehicle that receives this beacon could configure its OBU accordingly so that it will be able to reach the RSU. Note that the 802.11p does not require neither authentication nor association. Thus, the handoff delay is lower as the vehicle is ready to start communicating with the RSU much quicker than in the original WLAN standard. To enhance the privacy, the MAC address is no transmitted to the RSU as there is no association phase. However, RSUs are not able to identify a vehicle due to the lack of an association and de-association process. Therefore, while 802.11p standard is enough to provide fast handoffs it does not provide any kind of security.

Other proposals are based on the use of the IEEE 1609.4 standard [6] in order to optimize the handoff procedure. Two different channel types are described for use in this standard. The first type is the control channel, referred to as CCH, which is a single channel reserved for short, high-priority application and system control messages. The other type of channel is the service channel, or SCH, which has six different 10 MHz channels that support a wider range of applications and data transfer. Authors in [12] proposed a seamless handoff scheme for IEEE 802.11p where target RSUs can be identified by knowing the ID of the precedent RSU. OBUs are capable of triggering the handoff and they can also warn the current RSU that handoff is necessary by using the IEEE 802.11 disassociation message. Thus, the current RSU can forward data frames destined to the OBU to the next RSU which will pre-emptively buffer them. The new RSU will be also in charge of broadcasting a message so any entity in range could update their routing tables according to the new location of the requesting OBU. Once the OBU receives a WSA message from the new RSU, it will start receiving any buffered data frame. Figure 2 shows the message exchange process that provides the handoff functionality. However, this scheme suffers from inter-RSU interference as multiple RSU will be broadcasting beacons in the same frequency.

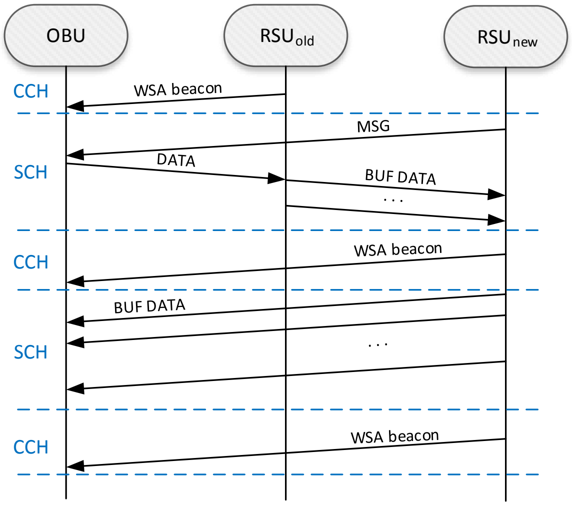

Figure 2: Message exchange sequence of the handoff process using 1609.4

Also based on the multi-channel capabilities of the IEEE 1609.4 standard [6], authors in [11] proposed a handoff algorithm. Following this algorithm, any OBU keeps track of any available service announced by a WSA message. Thus, OBUs build a table containing the provider service ID (PSID), priority and the received signal strength. The OBU current service is then verified and, based in the priority information, a SCH is chosen. To avoid collisions inside the control channel, RSUs use different time slots. Figure 3 shows the message exchange between two RSUs and one OBU.

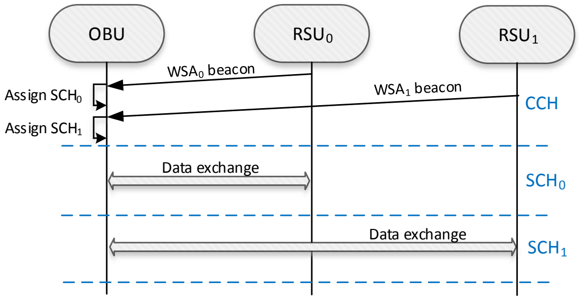

Figure 3: OBU Operation under multi-channel conditions using 1609.4

However, none of current 802.11p or 1609.4 based handoff mechanisms provides neither authentication nor access control which are essential to provide real-time applications (e.g. VoIP) in vehicular networks. Therefore, it is necessary to evaluate secure handoff standards proposed for traditional WLAN in vehicular scenarios.

3. SECURE HANDOFFS PROTOCOLS

At present, security protocols for wireless environments are designed in such a way that a mobile node needs to be authenticated at each access point when it moves around. Traditional 802.11 basically uses the EAP [7] as a generic authentication protocol which supports multiple authentication methods. In this section, we briefly describe four protocols that aim to optimize the EAP re-authentication, which indeed is a major contributor to the overall handoff latency.

3.1 IEEE 802.11i

IEEE 802.11i provides various security services: access control, data confidentiality, data integrity and data origin authenticity. After the RSU and the OBU make an association, they perform the authentication. However, the architecture and its authentication components, in an attempt to provide strong mutual authentication, ended up with a time consuming protocol with too many messages exchanges, and, therefore almost impracticable for V2I communications. IEEE 802.11i defines two methods for authentication: pre-shared key and centralized authentication. In the following, we describe the centralized authentication because it seems more suited for vehicular networks.

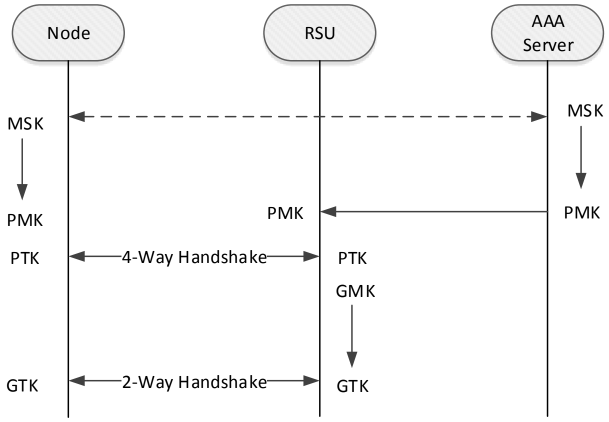

Figure 4: 802.11i protocol

In the centralized authentication method, IEEE 802.11i utilizes the IEEE 802.1X framework for access control. The protocol needs two keys: a Pairwise Transient Key (PTK) and a Group Transient Key (GTK). The PTK is used to protect unicast traffic both from the RSU to the OBU and from the OBU to the RSU. The GTK is used by the RSU to encrypt broadcast/multicast traffic sent to all OBUs currently in the BSS, and the OBUs need this key in order to decrypt the traffic. The sequence of the four-way handshake is shown in Figure 4. The basic operation mode consists in:

1. The OBU associates and then negotiates the security parameters used with the association.
2. The RSU authenticates the OBU.
3. A four-way key validation and distribution protocol is executed such that the PTK becomes available in the OBU and on the RSU.
4. The agreed-upon temporal keys are installed, using the negotiated cipher, and subsequent frames are protected.

It is worth noting that every message contains the identifier of the sender, a sequence number and a message number identifier. These elements, along with the fresh nonces, all serve the goal of defending against man-in-the-middle and replay attacks, while the MAC provides integrity protection on 4-way handshake messages calculated with PTK.

Thus, IEEE 802.11i pre-authentication reduces the overall handoff delay. However, it suffers from a series of issues. Mainly, each pre-authentication involves a full EAP authentication. Consequently, it implies a lot of signaling with the authentication server during each handoff. Moreover, the mechanism does not work when the involved RSUs belong to different distribution systems, which will be the case of a vehicular network.

3.2 IEEE 802.11r

IEEE 802.11r [4] overcomes most of the issues of the 802.11i by introducing a three level key hierarchy (started either from a Master Session Key (MSK) generated during an EAP authentication or a PSK) and a supporting architecture that allows the OBU to perform fast transition between the RSUs within the same so-called Mobility Domains without the need to run EAP authentication during each movement.

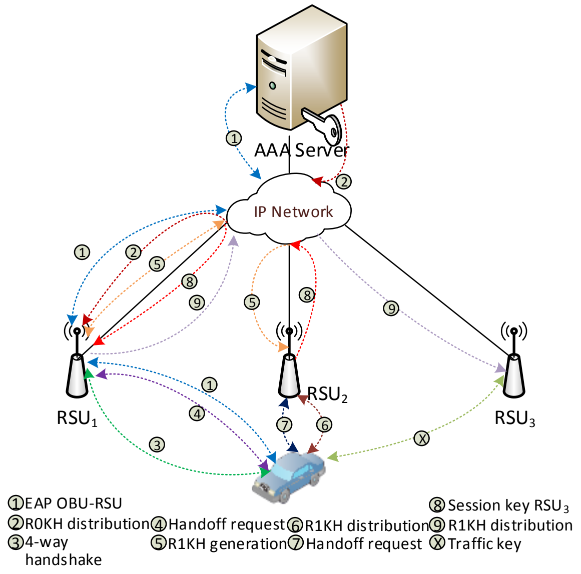

Figure 5: IEEE 802.11r handoff between APs

When an OBU first associates to an RSU of the vehicular network it performs a full authentication as it is done in IEEE 802.11i but extended with some IEEE 802.11r specific messages (see Fig. 5). The RSU$_0$ through which this full authentication is performed will play a special role during the upcoming handoff processes. Before leaving the current RSU, the OBU indicates the handoff and the identity of RSU$_1$ to the next RSU (through the current RSU or directly). The next RSU obtains an authentication key K from RSU$_1$. The OBU is able to generate K using some public information and the initial authentication key shared with RSU$_1$. The handoff is completed by running the 4-way handshake with the next RSU and deriving connection keys from K. In the standard IEEE 802.11r, some special roles are introduced. The RSU$_1$ plays the role of R0KH (Root$_0$ key holder) when generates RSU specific key (PMK-R1) from the MSK, and all access points including RSU$_1$ plays the role of R1KH (Root$_1$ key holder) when obtains the PMK-R1 and when derives the PTK. On the OBU's side, the same roles are present: S0KH (Supplicant$_0$ key holder) generates the access point specific keys and S1KH (Supplicant$_1$ key holder) derives the PTK with R1KH.

The main security-related benefits of the 802.11r are the opportunistic key caching and the elimination of the four-way handshake that traditionally followed re-association. Opportunistic key caching assumes that the necessary keying information would be made available to the target RSU either by some vendor-specific inter-RSU protocol or due to the fact that the four-way exchange was actually centrally controlled for all the RSUs.

Therefore, IEEE 802.11r reduces the handoff delay compared to IEEE 802.11i. However, IEEE 802.11r mechanism is not useful when the involved RSUs belong to different distribution systems. Basically, the reason is that the 802.11r handoff optimization mechanism is based on link-layer frames, which cannot operate across different subnets.

3.3 HOKEY

In the HOKEY standard [14], instead of performing full authentication with a remote authentication server each time an OBU re-authenticates to the vehicular network at different RSUs, HOKEY supports reusing the key generated at the initial authentication and shorten the delay of the re-authentication process. HOKEY's handoff process is depicted in Fig. 6.

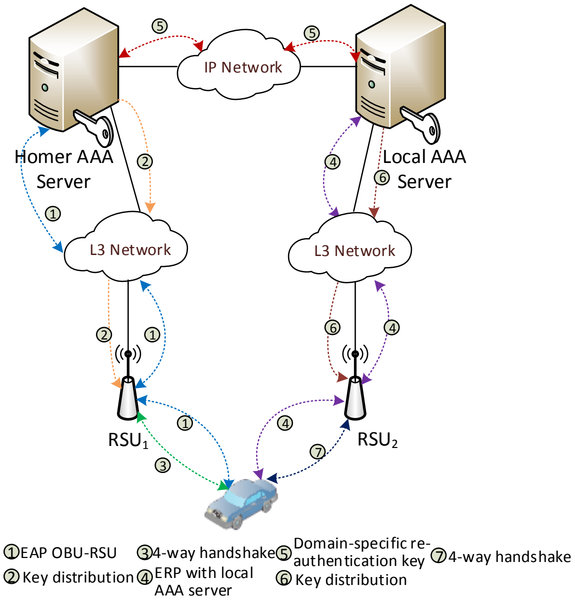

Figure 6: OBU handoff process using HOKEY

Basically, HOKEY main features are:

- During the initial authentication process, the client and the authentication server generates a handoff integrity key.
- When the client authenticates to another access point, it sends a request extending with a Message Authentication Code (MAC) using the handoff integrity key in a special EAP format (EAP-Initiate/Re-auth Packet).
- The authentication server, after verifying the MAC, responds to the access point with a fresh key generated in message EAP-Finish/Re-auth Packet such that the

mesh client is able to generate it, too, without any further communication.

The main benefit of HOKEY is that only one round trip message exchange is required between the OBU and the remote authentication server to perform the re-authentication. HOKEY was designed such that the operations performed during the re-authentication is independent of the initial EAP algorithm and the way of generating the first key. Furthermore, the HOKEY can handle different domains and it supports to install local authentication servers to shorten the round trip between the access point and the authentication server.

3.4 CAPWAP

Control and Provision of Wireless Access Points (CAPWAP) [10] was designed to provide interoperability between different vendors, allowing vehicles users to roam freely. It assumes all RSUs will be managed by a central authority. This central entity communicates with any OBU through a tunnel established between the central entity and the RSU which the OBU is associated with. During a handoff, the OBU associates with the next RSU and runs the 4-way handshake with the central entity (see Fig. 7).

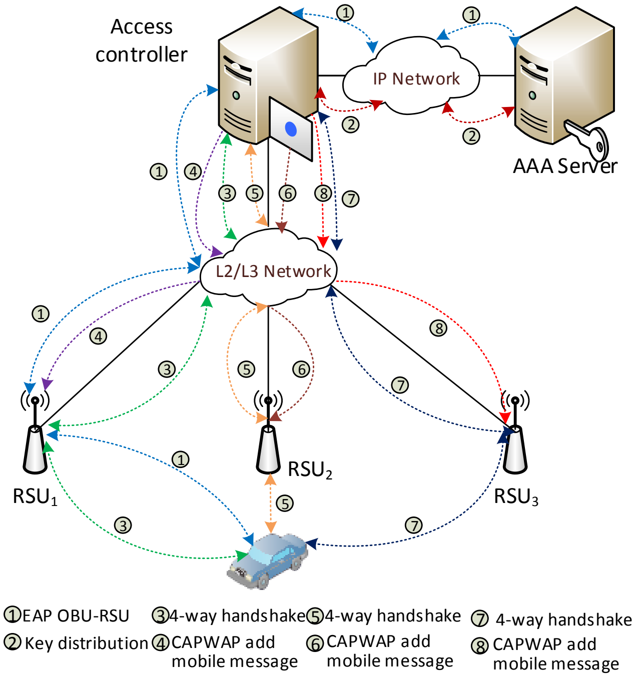

Figure 7: CAPWAP architecture: initial authentication with the AAA system followed by a transition between RSUs

The main advantage of CAPWAP is that no key material is stored at the RSUs. Hence, an attacker cannot obtain any keys by compromising an RSU. However, CAPWAP is extremely vulnerable to DoS attacks as there is no possibility to deny the access before a message arrives to the central access control enforcement unit. CAPWAP can also suffer from scalability issues as the central entity constitutes a single bottleneck.

4. PERFORMANCE EVALUATION

4.1 Analytic Evaluation

In this section, we compare relative handoff times for transitions within an RSU domain Let us define:
N = Number of round-trips required to perform a particular EAP method
T_{OBU} = Latency between the vehicle and RSU
T_{RSU} = Latency between two RSU
T_{AAA} = Latency between the vehicles and AAA server

As aforementioned, the original IEEE 802.11i handoff process uses the EAP method specific authentications which costs 2 round trips at minimum. Thus, the time to complete the EAP authentication is $2N(T_{OBU} + T_{AAA})$. Then, it will take T_{AAA} time to distribute the MSK to the RSU and finally the four way handshake between OBU and the RSU will take $4T_{OBU}$ time. Thus, the total 802.11i handoff time equals $2N(T_{OBU} + T_{AAA}) + T_{AAA} + 4T_{OBU}$.

HOKEY handoff latency includes a single round-trip execution which automatically delivers Handover Root Key. Thus HOKEY omits the time to distribute MSK to the RSU from 802.11i initial handoff. So, for HOKEY the handoff time is $2(T_{RSU}+T_{AAA})+4T_{OBU}$. On the other hand, 802.11r handoff consist of a handoff request from OBU to RSU, key distribution to the new RSU and final key handshake at the new RSU. It sums up to $2T_{AAA}+2T_{RSU}+2T_{OBU}$. CAPWAP is simple at application level, since it can use PMK; reside at centralized AC to derive multiple traffic keys. Thus, the handoff latency equals to $4(T_{OBU} + T_{RSU}) + T_{RSU}$. Table 1 shows the handoff latency per protocol.

Protocol	Handoff latency
802.11i	$2N(T_{OBU} + T_{AAA}) + T_{AAA} + 4T_{OBU}$.
802.11r	$2(T_{RSU} + T_{AAA}) + 4T_{OBU}$
HOKEY	$2T_{AAA} + 2T_{RSU} + 2T_{OBU}$
CAPWAP	$4(T_{OBU} + T_{RSU}) + T_{RSU}$.

Table 1: Handoff latency per protocol

4.2 Simulation

In order to compare the different protocols for the secure fast handoffs detailed in Section 3 we carried out a set of simulations to evaluate their performance. We implemented the different protocols and we have analyzed their performance on a single domain scenario. The test scenario designed for the performance evaluation is a highway vehicular scenario, where the highway has three lanes per direction, with the characteristics of the scenario depicted in Figure 8. This is an infrastructure scenario where a set of RSUs are deployed over a highway in an overlapped manner. Therefore there are no coverage blackouts in the road. All the RSUs are connected to a central router and this is also connected to a remote AAA server. The RSUs belong to the same subnet, so every handoff in the scenario is a layer 2 handoff.

We assume an intradomain scenario with a single infrastructure vendor. To perform the evaluation we used the ns-3 simulator version 3.17 [1]. We used the Simulation of Urban MObility (SUMO) [8] as a road traffic mobility simulator to generate the mobility traces used by ns-3 to model the mobility of the vehicular nodes.

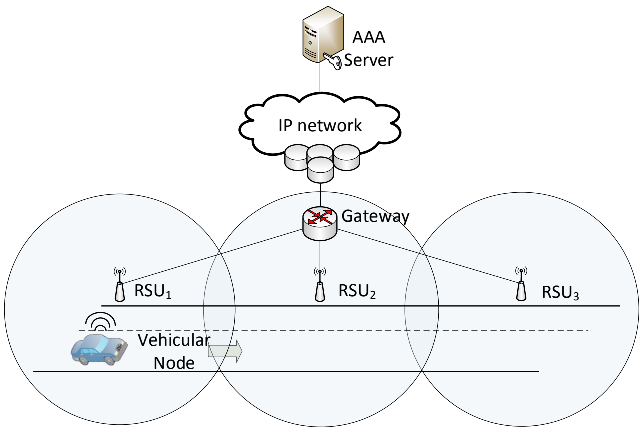

Figure 8: Reference scenario

Parameter Name	Value
Wired links	Bandwidth: 100Mbps Propagation delay: 5ms
AAA Server	Bandwidth: 1Gbps Propagation delay: 15ms
Propagation model	Two-Ray Ground
Interface queue	Droptail 50 packets
Distance between RSUs	200m
Packet size	1500 bytes
Highway scenario	2000 meters
Number of RSUs	10
Simulation Duration	100 s

Table 2: Simulation parameters

In Table 2 the simulation parameters are detailed. The simulation time is 100 seconds and the length of highway is 2000 metres. We used the MAC and PHY parameters from the 802.11p standard detailed in [5]. The MAC and PHY parameters used are depicted in Table 3. We used the 802.11 basic rate of 3 Mbps and the 802.11 data rate of 27 Mbps, thus control frames like ACKs or beacons are limited to be sent at 3 Mbps and data frames are sent to 27 Mbps The propagation model used is the Two-Ray Ground. We used four different speeds for the vehicles. These speeds range from 20 m/s to 35 m/s. The speeds are equally distributed between nodes with the same probability.

In the performance scenario we used different vehicular node densities to run the simulations. Different simulations were run varying the number of vehicles in the simulation (i.e., 1,25,50 and 100 vehicles), transmitting an UDP flow at constant rate of 100Kbps and the nodes' coverage range has been set to 250m.

Figures 9 and 10 represent the handoff disruption time associated to the authentication process. This disruption time is the handoff latency during the authentication added to the re-association latency (see Fig. 1). In Figure 9 is represented the handoff disruption times of the handoffs associated to all the vehicular nodes, as a function of the vehicular node density. In Figure 10 we can observe the average of these disruption times for each handoff protocol. In both figures we can observe CAPWAP, HOKEY and 802.11r have a significant reduction of the disruption time in contrast with the 802.11i approach. The difference between disruption times is higher when the vehicular density increases. While the 802.11i disruption time goes from 360 ms, in a single node scenario, to several seconds in a high density scenario, CAPWAP, HOKEY and 802.11r disruption times maintain a disruption time below 500 ms in most of the cases. However we can observe a different performance between CAPWAP and 802.11r approaches, and HOKEY solution. HOKEY performance is slight worse than CAPWAP and 802.11r. HOKEY is more affected by vehicular node density and therefore to the delay in the vehicular access network. This is mainly due to the fact that HOKEY requires more messages between a RSU and an OBU than CAPWAP and 802.11r.

Parameter Name	Value
Slot time	13 μs
SIFS	32 μs
RTS/CTS	Enabled
Rx Threshold	-82 dBm
CS Threshold	-86 dBm
Tx Power Level	35 dBm
Data rate	27 Mbps
Basic rate	3 Mbps
Intended range	250 m

Table 3: MAC and PHY 802.11 parameters

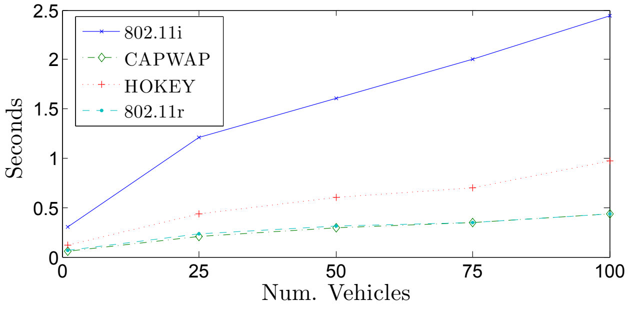

Figure 10: Average disruption time

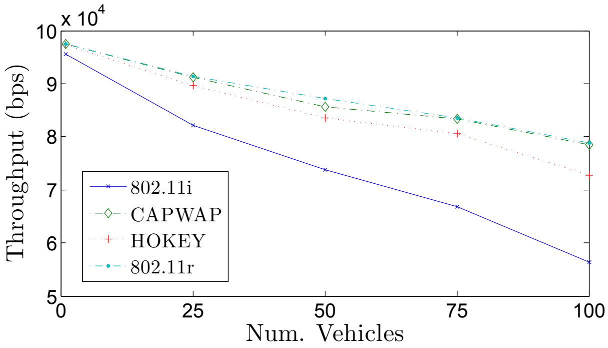

Figure 11: Average vehicular node throughput

Figure 11 represents the average throughput of the vehicles as a function of the vehicular node density. We can observe how the throughput is affected by the different disruption times of each protocol. We can observe that while using 802.11i protocol the throughput decreases drastically with the vehicular node density, fast handoff protocols per-

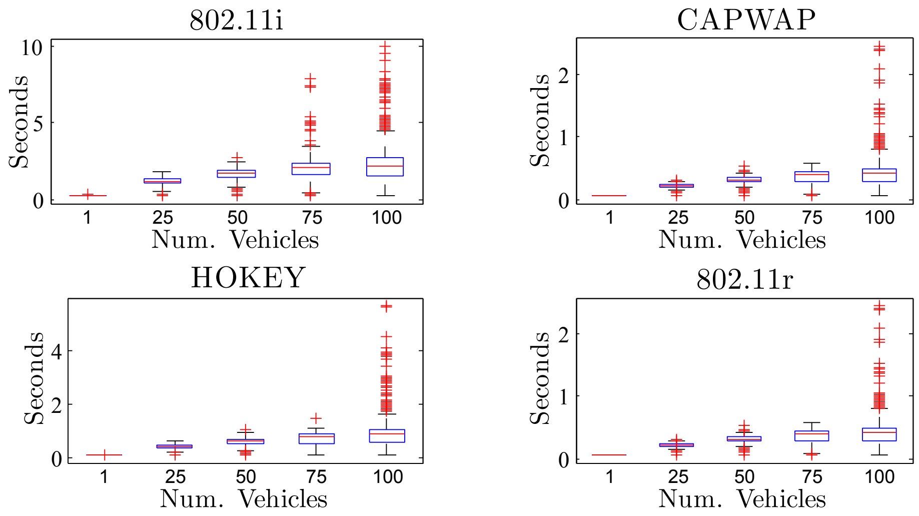

Figure 9: Handoff disruption time

form much better in saturated networks. Again, we can observe that HOKEY performance in terms of throughput is much worse than CAPWAP and 802.11r protocols when the vehicular node density increases.

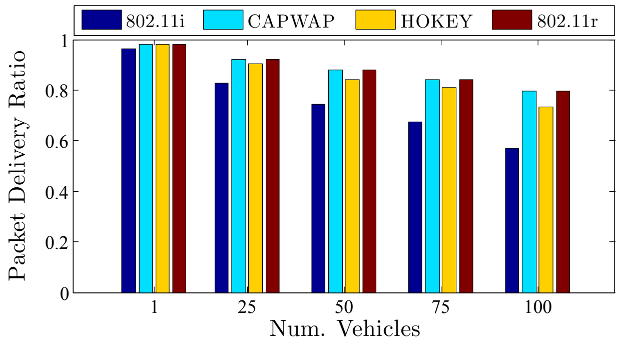

Figure 12: Packet delivery ratio

In Figure 12 we can observe the packet delivery ratio for each protocol. This packet delivery ratio behaves similarly to the throughput, being CAPWAP and 802.11r the most reliable solutions, very close to HOKEY protocol.

5. CONCLUSIONS

Fast and secure handoff protocols are essential for VANETs to support Internet based real-time applications (e.g., video-streaming, Internet browsing, online gaming, etc.) using V2I communication. Getting access to the network infrastructure must be controlled and only authorized users should be able to use it. However, maintaining ubiquitous connectivity remains a challenge due to both high vehicle speed, and non-homogeneous nature of the network access infrastructure. Authentication protocols incurs in a not-negligible delay which can result in packet losses and other issues during handoffs. Hence, a fast and secure handoff scheme is essential. In this article we detailed the most important secure handoff protocols, i.e., 802.11i, CAPWAP, HOKEY and 802.11r.

Moreover, we have evaluated the performance of these protocols. We have shown that fast handoffs protocols such as HOKEY, CAPWAP and 802.11r perform much better than the 802.11i protocol. Among the fast handoff protocols, CAPWAP and 802.11r perform better than HOKEY in a vehicular scenario. The main reason is that in a vehicular scenario, the high density of the vehicular nodes turns the access network into a bottleneck. HOKEY sends more messages, during the authentication process, between the RSU and the OBU using the vehicular access network, than CAPWAP and 802.11r. Therefore CAPWAP and 802.11r perform better in saturated vehicular networks. However, while HOKEY may have worse intradomain handoff performance than CAPWAP and IEEE 802.11r, it really shines when it comes to cross-domain handoffs. No other protocol supports handing credentials from one authenticator to another, whether that authenticator is in the same domain or a remote one. With high latencies local handoff using a local AAA server that has cached your credentials is a significant improvement in wireless handoff times. However it is more feasible in a vehicular network to replicate AAA servers throughout the infrastructure than improve the performance of the access network.

6. ACKNOWLEDGMENTS

This work has been supported partially by the Spanish Research Council with Project TEC2011-26452 (SERVET), by FPU grant AP2010-0244, by Spanish Ministry of Science and Education with Project CONSOLIDER CSD2007-00004 (ARES), by Generalitat de Catalunya with Grant 2009 SGR-1362 to consolidated research groups and with the support from the SUR (Secretaria d'Universitats i Recerca) of the DEC (Departament d'Economia i Coneixement), and by the European Social Funds.

7. REFERENCES

[1] NS-3 Network Simulator. `http://www.nsnam.org/`.
[2] 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. *IEEE Std 802.11F-2003*, pages 1–67, 2003.

[3] 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. *IEEE Std 802.11i-2004*, pages 1–175, 2004.

[4] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition. *IEEE Std 802.11r-2008*, pages 1–126, 2008.

[5] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. *IEEE Std 802.11p-2010*, pages 1–51, 2010.

[6] IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation. *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006)*, pages 1–89, 2011.

[7] B. Aboba, D. Simon, and P. Eronen. Extensible Authentication Protocol (EAP) Key Management Framework. RFC 5247 (Proposed Standard), Aug. 2008.

[8] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz. SUMO - Simulation of Urban MObility: An Overview. In *SIMUL 2011, The Third International Conference on Advances in System Simulation*, pages 63–68, Barcelona, Spain, October 2011.

[9] M. Brown and R. Housley. Transport Layer Security (TLS) Authorization Extensions. RFC 5878 (Experimental), May 2010.

[10] P. Calhoun, M. Montemurro, and D. Stanley. Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification. RFC 5415 (Proposed Standard), Mar. 2009.

[11] W. Cho, M. Kim, S. W. Lee, and H. seo Oh. Implementation of handover under multi-channel operation in IEEE 802.11p based communication systems. In *2011 International Conference on ICT Convergence (ICTC)*, pages 151–155, 2011.

[12] J. Choi and H. Lee. Supporting handover in an IEEE 802.11p-based wireless access system. In *Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking*, VANET '10, pages 75–80, New York, NY, USA, 2010. ACM.

[13] T. Clancy. Secure handover in enterprise WLANs: CAPWAP, HOKEY, and IEEE 802.11r. *Wireless Communications, IEEE*, 15(5):80–85, 2008.

[14] T. Clancy, M. Nakhjiri, V. Narayanan, and L. Dondeti. Handover Key Management and Re-Authentication Problem Statement. RFC 5169 (Informational), Mar. 2008.

[15] A. DeKok and A. Lior. Remote Authentication Dial In User Service (RADIUS) Protocol Extensions. RFC 6929 (Proposed Standard), Apr. 2013.

[16] G. Jeney, L. Bokor, and Z. Mihaly. GPS aided predictive handover management for multihomed NEMO configurations. In *Intelligent Transport Systems Telecommunications,(ITST),2009 9th International Conference on*, pages 69–73, 2009.

[17] R. Marques, E. Araújo, and A. Zúquete. Fast 802.11 handovers with 802.1X reauthentications. *Security and Communication Networks*, 4(3):267–283, 2011.

[18] A. Mishra, M. Shin, and W. Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. *SIGCOMM Comput. Commun. Rev.*, 33(2):93–102, Apr. 2003.

[19] A. Tabassam, H. Trsek, S. Heiss, and J. Jasperneite. Fast and seamless handover for secure mobile industrial applications with 802.11r. In *Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on*, pages 750–757, 2009.