EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Analytical efficiency evaluation of a network mobility management protocol for Intelligent Transportation Systems

Nerea Toledo[1*], Marivi Higuero[1], Jasone Astorga[1], Marina Aguado[1] and Xavier Lagrange[2]

Abstract

One of the major concerns in an Intelligent Transportation System (ITS) scenario, such as that which may be found on a long-distance train service, is the provision of efficient communication services, satisfying users' expectations, and fulfilling even highly demanding application requirements, such as safety-oriented services. In an ITS scenario, it is common to have a significant amount of onboard devices that comprise a cluster of nodes (a mobile network) that demand connectivity to the outside networks. This demand has to be satisfied without service disruption. Consequently, the mobility of the mobile network has to be managed. Due to the nature of mobile networks, efficient and lightweight protocols are desired in the ITS context to ensure adequate service performance. However, the security is also a key factor in this scenario. Since the management of the mobility is essential for providing communications, the protocol for managing this mobility has to be protected. Furthermore, there are safety-oriented services in this scenario, so user application data should also be protected. Nevertheless, providing security is expensive in terms of efficiency. Based on this considerations, we have developed a solution for managing the network mobility for ITS scenarios: the NeMHIP protocol. This approach provides a secure management of network mobility in an efficient manner. In this article, we present this protocol and the strategy developed to maintain its security and efficiency in satisfactory levels. We also present the developed analytical models to analyze quantitatively the efficiency of the protocol. More specifically, we have developed models for assessing it in terms of signaling cost, which demonstrates that NeMHIP generates up to 73.47% less signaling compared to other relevant approaches. Therefore, the results obtained demonstrate that NeMHIP is the most efficient and secure solution for providing communications in mobile network scenarios such as in an ITS context.

Keywords: Network mobility, Security, Confidentiality, Integrity, Signaling overhead, Host identity protocol

1 Introduction

The rapid progress in wireless communication standards and networking technologies has made it easier to provide communication services with increasing demands in sophisticated scenarios such as entire moving networks, where continuous and optimal Internet access is required. An example of such a scenario is an Intelligent Transportation System (ITS) as illustrated in Figure 1.

From a communications point of view, a vehicle in the ITS context is regarded as a mobile network. Figure 1 shows a vehicle in the ITS context equipped with several nodes, called mobile network nodes (MNNs). These MNNs communicate with correspondent nodes (CNs) located in an outside network, typically, on the Internet. These communications are commonly managed by an entity known as a Mobile Router (MR), which functions as the anchor point to the Internet of the mobile network (see Figure 1 for more details). The use of an MR to manage all the communications between the vehicle and the outside network reduces the signaling cost and the overall management complexity. In this context, the MR is in charge of managing the mobility of the entire network. This mobility management has a twofold goal: to provide continuous communication without service disruption

*Correspondence: nerea.toledo@ehu.es
[1] Department of Communication Engineering, University of The Basque Country, Alameda Urquijo s/n, 48013 Bilbao, Spain
Full list of author information is available at the end of the article

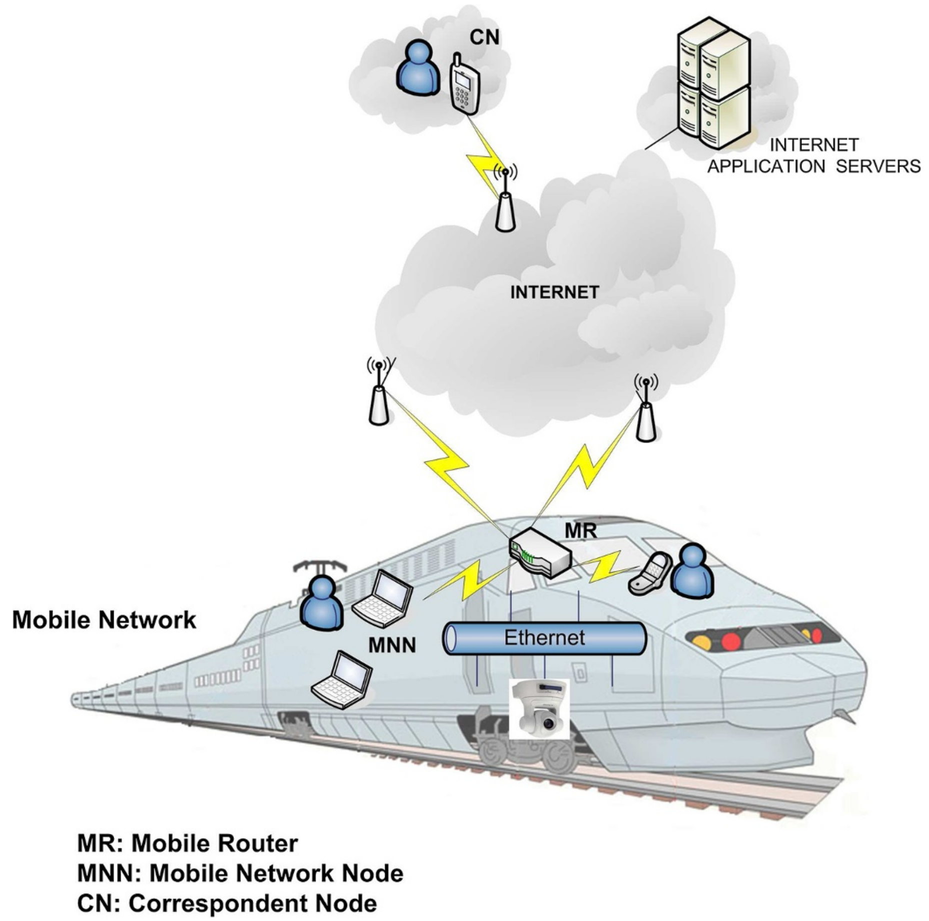

Figure 1 The ITS context.

due to mobility events; and to allow reachability of MNNs in the vehicle from any point on the Internet.

MNNs can be onboard user devices or devices in charge of controlling and monitoring the operation of the vehicle or end user devices such as smartphones or laptops. Such devices demand anytime-anywhere connectivity to the Internet. Moreover, Internet-based applications are considered beneficial for safety, and fundamental for non-safety purposes [1], and as such, MNNs should be reachable from the Internet. In fact, Internet provisioning not only provides support for diverse services for travelers and the crew, but also improves onboard diagnostic systems that support ITS operational services.

In this scenario where there will be a wide variety of applications, new protocols and procedures to be introduced have to be efficient and support the requirements those applications impose. Therefore, efficiency in terms of signaling cost of the network mobility management procedure enhances the performance of user applications, while facilitating the introduction of future network services and thus, a successful penetration of ITS technologies. The efficiency becomes even more critical with the presence of wireless links, as is the case with mobile networks and an ITS scenario, because in wireless links both the bandwidth and communication resources are generally limited.

Another essential aspect that has to be addressed by the protocols to be introduced in the ITS context is the security support. ITS operational services include data related to the operation and control of the vehicle's engine and machinery, and so, these data are considered critical for the correct operation of the vehicle. If security attacks, such as misconfigurations of the machinery of the vehicles, erroneous acquisition of the control information of the vehicles, problems in the remote control of the engines, bogus information provisioning from an outside network are prone to occur, safety could be at stake.

To ensure the required security level in an ITS scenario, not only user data, but also the network mobility management process itself must be protected to guarantee the required security properties. If the network mobility management procedures are not secured, ongoing communication could be broken, the establishment of new communication could be prevented, or the mobile network could be isolated.

Although the MIPv6-based NEMO BS [2] solution is the standardized solution for managing network mobility, it presents shortcomings which are detailed in Section 2. To overcome these shortcomings, other solutions exist, which assume alternative protocols to MIPv6 such as the Host Identity Protocol (HIP) [3], which is known to be the most complete protocol because it addresses security and mobility management while also providing optimal routing. As a result, we have designed an efficient and secure network mobility management protocol based on HIP for ITS scenarios, the NeMHIP protocol. In this article, we introduce the NeMHIP protocol and describe the developed model for analytically evaluating the efficiency of our approach and demonstrate that the introduction of security features does not penalize the efficiency. Furthermore, we have compared obtained results with other approaches that also consider HIP to cover network mobility, positioning our solution. Obtained results show that NeMHIP is a lightweight approach and a suitable solution to be applied in the ITS context, while providing the desired level of security.

The rest of this article is organized as follows. In Section 2, we present the most relevant approaches proposed thus far for addressing network mobility scenarios. Based on this overview, in Section 3 we present our approach, NeMHIP, which is designed to efficiently and securely manage network mobility in ITS scenarios. Section 4 describes the analytical models developed and the assessment conducted to demonstrate that NeMHIP fully satisfies the efficiency requirement of the ITS context because the generated signaling cost over the wireless link is reduced compared with that of other approaches [4]. In Section 5, we present our concluding remarks.

2 Related study

Currently, NEMO BS (RFC 3963) is the solution adopted by the ETSI and ISO standardization bodies to support network mobility. It is based on MIPv6 and provides session continuity to every node located within the mobile network when the network moves. It also ensures that every onboard node is always reachable from the Internet.

In the NEMO BS protocol, it is assumed that the mobile network has a Home Network, where it resides when it is not moving. Since the moving network is part of the Home Network, its addressing structure is part of the address block assigned to the Home Network. In addition, the MR has a unique Home Address configured from a prefix advertised by its Home Agent (HA).

In NEMO BS, signaling messages for managing the mobility are exchanged with the HA, instead of directly with a node (the CN). Furthermore, data packets with a destination within the mobile network traverse the HA and vice versa. This type of routing is called *dog-leg routing* and is considered to be suboptimal, because packets travel over longer paths resulting in higher delays than necessary. Because of this, several approaches have been released to provide route optimization (RO). In RO schemes, packets do not traverse the HA, but are exchanged following an optimal path between the CN and MR.

Owing to the need of both efficiency and security support in the ITS context, the simultaneous introduction of both RO and security support is required. Nevertheless, this is the most challenging scenario because a secure relationship between the MR and CN cannot be assumed *a priori*. On the one hand, solutions addressing this problem have proposed add-ons to the NEMO BS protocol, resulting in a conglomeration of procedures and frameworks that are complex to manage. On the other hand, there are solutions also based on NEMO BS that rely on exchanging information between the CN and MR traversing the HA to guarantee security. Besides the lack of a preestablished security association (SA) between the MR and CN, the use of IP addresses to identify and locate a node is also a major concern. Furthermore, IP addresses are commonly used in the definition of security policies. Consequently, in a mobile scenario where IP addresses change constantly, this issue becomes an even greater problem.

Apart from the solutions based on NEMO BS, another wave of proposals exist aimed at enhancing the drawbacks of the NEMO BS protocol by considering alternative mobility management protocols, such as Session Initiation Protocol, LIN6, or HIP. These mobility management protocols aim to address the shortcomings of NEMO BS from the outset. Of the aforementioned alternatives, HIP is the only solution that solves the suboptimal routing problem while providing a complete security framework in the defined mobility management procedures. Therefore, we have focused on HIP to design an efficient and secure network management protocol.

The cornerstone of HIP is separating a node's location and identifier by introducing a new cryptographic namespace (public–private key pair) known as the Host Identity Tag (HIT), to identify the nodes. Therefore, HIP can be seen as a new layer between the network and transport layers, which maintains the mapping between a node's identifier and its location. The HIP protocol defines a handshake to establish SAs. Once SAs have been established, the IPsec Encapsulating Security Payload (ESP) protocol is adopted to transport data securely. Therefore, two different security planes can be distinguished: (1) security properties related to the HIP signaling itself (signaling plane); and (2) security features required for data transport (data plane). Overall security functionalities include mutual authentication achieved by means of the Hash-based Message Authentication Code (HMAC), integrity protection also achieved through the HMAC field and data confidentiality protection achieved through the IPsec ESP.

HIP also defines how to update the SAs; i.e., the protocol addresses rekeying and mobility needs. This update is achieved by means of a handshake called UPDATE, with its major goals being to notify the new location of the node (new IP address) and/or request new keys when necessary.

The provision of network mobility support based on HIP is not straightforward because HIP is built over an end-to-end paradigm. In this context, one of the main issues is manageability. Independently managing all end-to-end associations between MNNs and CNs results in increased complexity and significant cost. For this reason, the HIP-based network mobility management solutions proposed thus far [4-6] are based on the *delegation of signaling rights* concept [7]. This concept refers to the procedure in which a node authorizes another node to perform signaling procedures on its behalf. In a network mobility scenario, the MNNs delegate their signaling rights to the MR, to reduce the signaling cost and improve manageability. Therefore, the MR is in charge of managing the rekeying agreements on behalf of the MNNs. This approach presents security vulnerabilities when ensuring the secrecy of information that should not be revealed to third parties. Furthermore, the CN verifies that the MR is authorized to send signaling messages on behalf of the MNN by means of checking the authorization ticket and the end-to-end key provided in the delegation of signaling rights process. However, it does not authenticate the MR, and since the MNN cannot deny the MR the permission to further give the authorization ticket not it can prevent from distributing the key used in the MNN–CN authentication process, a dishonest node could end up having the needed data to mount attacks on the mobility management process. As a result, the ongoing communications could be broken and new communications could not be established with onboard nodes. In addition, the keys agreed upon are used not only to protect the signaling plane, but also the data plane (IPsec ESP), and thus, if these keys are compromised, confidentiality and integrity of the data could also be endangered.

On the other hand, in an ITS context it is common to have different wireless access technologies deployed. Therefore, the mobility of the mobile network may result in access technology changes (vertical handovers). As a result of these technology changes, path characteristics such as throughput, link delay, and so on may vary drastically. In HIP, IPsec ESP is used to protect data and the ESP anti-replay window is mandatory [8]. Variations in the above-mentioned path characteristics together with the packet loss inherent in a handover process may result in receiving packets over the new communication access technology with sequence numbers outside the ESP anti-replay window, and consequently, packet discards. As a result, it is critical to rekey the associations whenever a handover occurs [9].

The demand of being MNNs oblivious to mobility events to simplify the handover procedures comes face-to-face with the need to rekey the end-to-end association when a mobility event that results in changing the IP address occurs. Since MNNs do not know that a mobility event has happened, they will not rekey the end-to-end associations, and so, security vulnerabilities related to mobility would still be present. A straightforward solution would be to inform the MNNs to conduct end-to-end SA updates, but this would result in an unmanageable signaling cost; i.e., the advantages of delegating signaling rights would be lost.

In this context, we have defined the NeMHIP protocol, which solves the problem of rekeying whenever a mobility event takes place and manages the end-to-end SAs without significantly increasing the signaling cost.

3 The NeMHIP network mobility management protocol

The NeMHIP protocol has been designed to address the need to provide an efficient and secure network mobility management solution for ITS scenarios. The main goal of the protocol is to ensure security support for the network mobility management process and also for the end-to-end data exchange. In addition, efficiency in terms of signaling cost is also achieved using the NeMHIP protocol. The basis of the NeMHIP protocol has been published in [10]. In [11], we presented the design goals and procedures of the protocol and evaluate the performance of user applications. This article completes the work already published, since it describes efficiency-related aspects of the protocol modeling them analytically and compares our approach with other solutions proposed in the literature, positioning our contributions.

The NeMHIP integrates within a single framework the mobility management of the entire network and the end-to-end security properties. To do so, in NeMHIP the MR is in charge of both managing the mobility and initiating a procedure to rekey the end-to-end associations when necessary, but without needing end-to-end signaling exchanges. Therefore, NeMHIP has the same advantages as a solution based on the delegation of signaling rights. However, since it is not based on the concept of delegation of signaling rights, it mitigates the security vulnerabilities of this approach. In other words, the NeMHIP protocol does not introduce any security vulnerabilities but provides the same advantages as a solution based on the delegation of signaling rights.

3.1 NeMHIP procedures

In this section, we present the core procedures defined by the NeMHIP protocol: the NeMHIP Association Establishment and the NeMHIP Association Update.

3.1.1 NeMHIP association establishment

It should be pointed out that as a previous step in establishing a NeMHIP association between a node on the Internet (CN) and a node in a mobile network (MNN), these MNNs should be reachable from the Internet. The ability to reach MNNs is the result of registering them with a RendezVous Server (RVS), which stores their identifier and location information. Further details on the registration process can be found in our previous work [12]. In describing the two core procedures mentioned above (NeMHIP Association Establishment and Update), we assume that the MNNs are already registered with the RVS.

When an onboard node (MNN) wishes to communicate securely with a node on the Internet (CN) or vice versa, a NeMHIP association must be established. The case in which a CN initiates the communication is more challenging because it must know the location of the MNN beforehand. This case is described next. With the goal of clarifying the description of packets defined by the NeMHIP protocol, Table 1 shows the notation and terminology used in the definition of exchanged packets.

A NeMHIP association is initiated by an $I1$ packet sent by the CN to the RVS with the source and destination identifiers (*HIT.CN* and *HIT.MNN*), respectively. The RVS intercepts this $I1$ packet and checks for the destination IP address (*IP.MNN*) to route the packet to the MNN. The RVS knows that the MNN is located in a mobile network because the identifier of the MR (*HIT.MR*) is stored with the identifier of the MNN (*HIT.MNN*) and its locator. With this information, the RVS generates an $I1'$ packet including the identifier of the MR there in.

Table 1 Exchanged parameters

Parameter	Meaning
HIT_{node}	Host Identity Tag of entity *node*, i.e. *Hash(Host Identity)*
g	Diffie Hellman primitive root
g^X	g^X modulus p, where p is a prime number
HIP_{trans}	Supported HIP cryptographic suite (AES-CBC with HMAC-SHA1)
ESP_{trans}	Supported ESP cryptographic suite (AES-CBC with HMAC-SHA1)
$puzzle_{node}$	Cryptographic challenge introduced by entity *node*
sol_{node}	Solution of the puzzle introduced by entity *node*
$ESP_{INFO_{node1,node2}}$	Security Parameter Index (SPI) value and keying material index
	to be used between *node1* and *node2*
K^{+}_{node}	Public key of the entity *node*
K^{-}_{node}	Private key of the entity *node*
$K_{node1,node2_e}$	Encryption key shared between entities *node1* and *node2*
$K_{node1,node2_i}$	Integrity key shared between entities *node1* and *node2*
$K_{node1,node2_i}$	Integrity or encryption key shared between entities *node1* and *node2*
m	Refers to the message over which the HMAC is computed, i.e., all the packet
	except the HMAC parameter itself and the parameters that follow it
$HMAC(K_{node1,node2_i}\|m)$	Hashed Message Authentication Code
LOCATOR	New IP address where the mobile network is reachable
SEQ	Sequence Number
N	Nonce
ECHO(N)	The echo of the received nonce

Once the NeMHIP association has been triggered with the $I1$ and $I1'$ packets, a double authenticated DH exchange is conducted between the MR and CN in packets $R1'$, $I2'$, and $R2''$. This double authenticated DH exchange is the most significant procedure of NeMHIP because it is needed to agree upon independent and different keying material between the MNN and the CN and between the MR and the CN. Hence, the fields required by the authenticated DH are included in these packets. In addition, a challenge–response procedure is included to protect the responder from denial-of-service attacks. To this end, the MNN and the MR challenge the CN with independent puzzles. That is, upon complexion of the NeMHIP association establishment process, two independent and parallel SAs are established, one between the MR and the CN that is used to protect mobility management messages and the other between the MNN and the CN, to protect user data messages.

Figure 2 shows the packets exchanged in establishing a NeMHIP Association when the CN initiates the communication. Table 2 details the format of the packets exchanged during NeMHIP Association Establishment.

Upon completion of the NeMHIP Association Establishment exchange, the MNN shares keying material with the CN, while the MR also shares keying material with the CN. It should be noted that both keying materials are unknown to each other and the CN treats them as independent keying materials. Encryption and integrity protection keys are derived from these keying materials based on an index selected by the involved parties. That is, although the MR takes part in the NeMHIP Association Establishment the CN agrees on a set of keys with the

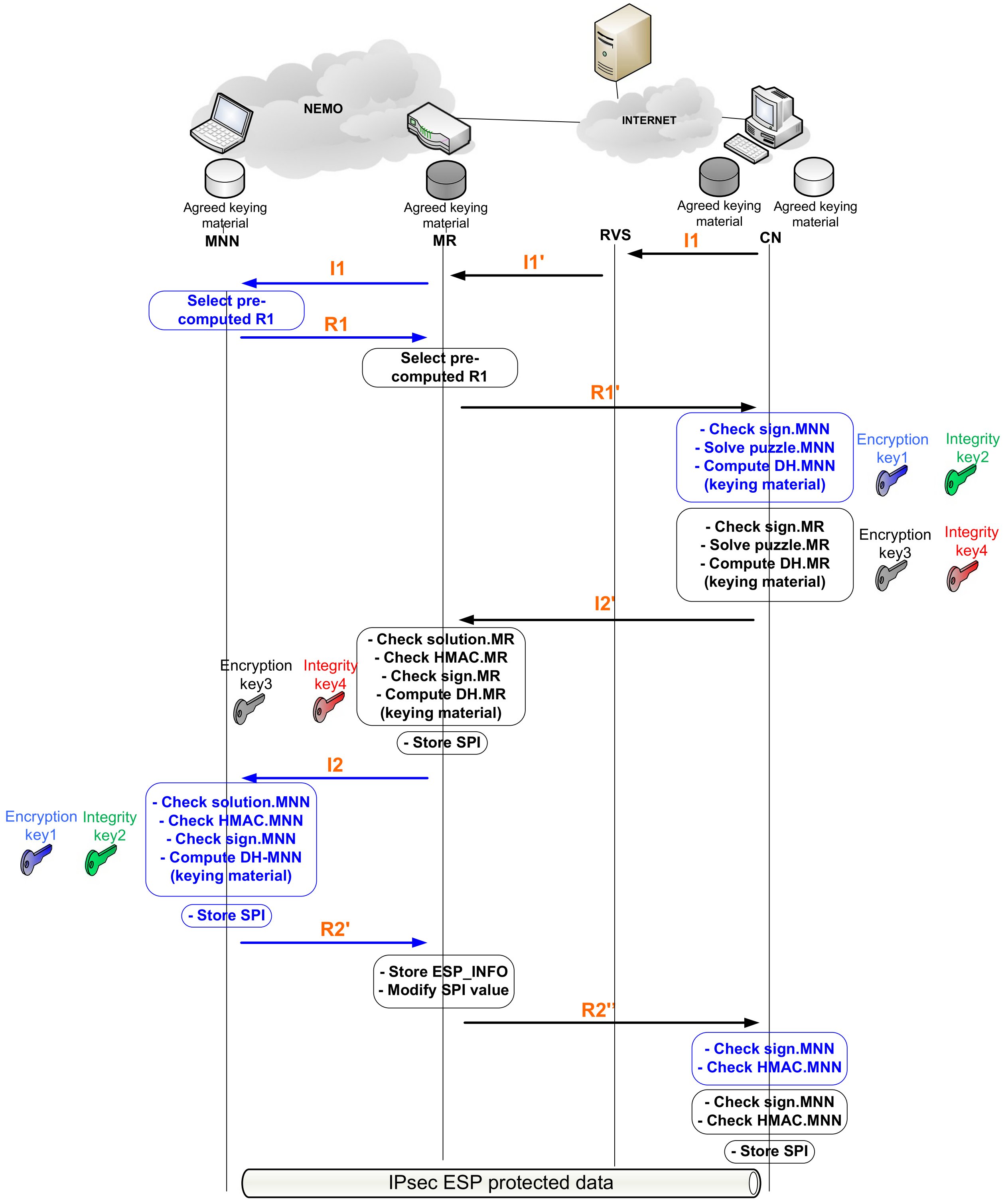

Figure 2 NeMHIP association establishment.

Table 2 Definition of the packets exchanged during NeMHIP association establishment

Packet	Direction	Fields
I1	$CN \rightarrow RVS$	HIT_{MNN}, HIT_{CN}
I1′	$RVS \rightarrow MR$	$HIT_{MR},HIT_{CN},HIT_{MNN},HIT_{CN}$
I1	$MR \rightarrow MNN$	HIT_{MNN}, HIT_{CN}
R1	$MNN \rightarrow MR$	$\{HIT_{CN}, HIT_{MNN}, puzzle_{CN}, g^{Y}, HIP_{trans_{CN}},$ $K^{+}{}_{MNN}\}_{K^{-}{}_{MNN}}$
R1′	$MR \rightarrow CN$	$\{HIT_{CN}, HIT_{MR}, \{HIT_{CN}, HIT_{MNN}, puzzle_{CN}, g^{Y}$ $HIP_{trans_{CN}}, K^{+}{}_{MNN}\}_{K^{-}{}_{MNN}} puzzle_{MR}, g^{X}, HIP_{trans_{MR}},$ $K^{+}{}_{MR}\}_{K^{-}{}_{MR}}$ $\{\{HIT_{MR}, HIT_{CN}, HIT_{MNN}, HIT_{CN},$ $sol_{MNN}, g^{W},$
I2′	$CN \rightarrow MR$	$HIP_{trans_{CN}}, \{ESP_{INFO_{CN,MNN}}\}_{K_{CN,MNN_e}},$ $HMAC(K_{CN,MNN_i}\|m)\}_{K^{-}{}_{CN}}, \{sol_{MR}, g^{Z}, HIP_{trans_{CN}},$ $ESP_{INFO_{CN,MR}}, ESP_{trans_{MNN}}, ESP_{INFO_{CN,MNN}},$ $HMAC(K_{CN,MR_i}\|m)\}_{K_{CN,MR_e}}\}_{K^{-}{}_{CN}}$ $\{HIT_{MNN}, HIT_{CN},$ $\{sol_{MNN}, g^{W},$
I2	$MR \rightarrow MNN$	$HIP_{trans_{CN}}, ESP_{trans_{MNN}}\{ESP_{INFO_{CN,MNN}}\}_{K_{CN,MNN_e}},$ $HMAC(K_{CN,MNN_i}\|m)\}_{K^{-}{}_{CN}}\}_{K^{-}{}_{MR}}$
R2′	$MNN \rightarrow MR$	$\{HIT_{CN}, HIT_{MNN}, \{ESP_{INFO_{CN,MNN}},$ $HMAC(K_{CN,MNN_i}\|m)\}_{K_{CN,MNN_e}}, ESP_{INFO_{CN,MNN}},$ $HMAC(K_{MR,MNN_i}\|ESP_{INFO_{CN,MNN}})\}_{K^{-}{}_{MNN}}$
R2″	$MR \rightarrow CN$	$\{HIT_{MR}, HIT_{CN}, HIT_{CN}, HIT_{MNN}, \{ESP_{INFO_{CN,MNN}},$ $HMAC(K_{CN,MNN_i}\|m)\}_{K_{CN,MNN_e}}, NAT\_ESP_{INFO},$ $HMAC(K_{CN,MR_i}\|m)\}_{K^{-}{}_{MR}}$

MNN, and another set of keys with the MR, so end-to-end integrity and confidentiality are ensured.

From this point, data are exchanged securely between the MNN and the CN using IPsec ESP.

3.1.2 NeMHIP association update

In the same way as the base HIP protocol, NeMHIP also includes a procedure to update the established NeMHIP associations. The procedure defined for doing so is presented next.

It should be noted that a NeMHIP association is established between a CN and an MNN. As these nodes share a security context, either of them can request an association update when necessary. Furthermore, mobility events due to the movement of the mobile network also result in updating NeMHIP associations. In this case, the MR is the node initiating the update process because it is in charge of managing the mobility of the entire network. Therefore, apart from the CN and the MNN, the MR can also trigger a NeMHIP Association Update. Moreover, since updates triggered by the MR are more critical because communication continuity is at stake, we focus on them in this section.

To maintain ongoing communications, mobility events that result in changing the point of attachment to the Internet must be notified to the CNs that are communicating with the MNNs. Furthermore, the new location of the mobile network has to be updated in the RVS to ensure that the MNNs continue to be reachable. As previously mentioned, the established associations should be rekeyed when a mobility event occurs. Therefore, the MR should not only inform the CN of its new location, but also of the new index to derive new keys. At the same time, the MR informs the MNN of the new index that it should use to derive new end-to-end keys. In this way, there is no need to exchange end-to-end signalling messages between the MNN and the CN to update the NeMHIP association. Through this notification, the MNN and the CN both have the keying material index synchronized and data can be exchanged in a protected manner using the new keys. This procedure is possible because the MR is aware of the selected indexes exchanged in the NeMHIP Association Establishment process. Figure 3 shows the update signaling during a handover by the mobile network.

Details of the packet formats are given in Table 3.

It should be noted that in the update process between the MR and the MNN, two messages are exchanged ($NOTIFY\_UPDATE$) and ($NOTIFY\_UPDATE_{ACK}$), while the update process between the MR and the CN requires three messages. This is because in the update process between the MR and the CN, the new IP address to be used is provided. This notification demands verification of the IP address, which is conducted in messages $UPDATE2$ and $UPDATE3$ by means of a nonce-echoing procedure. However, the new IP address is not sent to the MNN; thus, no verification is required. Therefore, only two messages are exchanged instead of the three between the MNN and the MR.

3.2 Security properties of NeMHIP

In this section, we briefly introduce the security properties of our protocol.

NeMHIP has been designed with the goal of providing a complete security framework for communications in ITS scenarios. However, it is common to have penalizations in the efficiency as a result of including security features. Therefore, in this study, we have considered these concerns when designing the strategy to introduce security aspects to the protocol. In fact, the NeMHIP protocol ensures security properties not only to the end-to-end data exchanges, but also to the network mobility management message exchanges.

In our approach, we have integrated the mobility management of the entire network and the end-to-end security provisioning functionalities in a single framework. By doing so, we ensure the same advantages as a delegation of signaling rights approach while avoiding the security

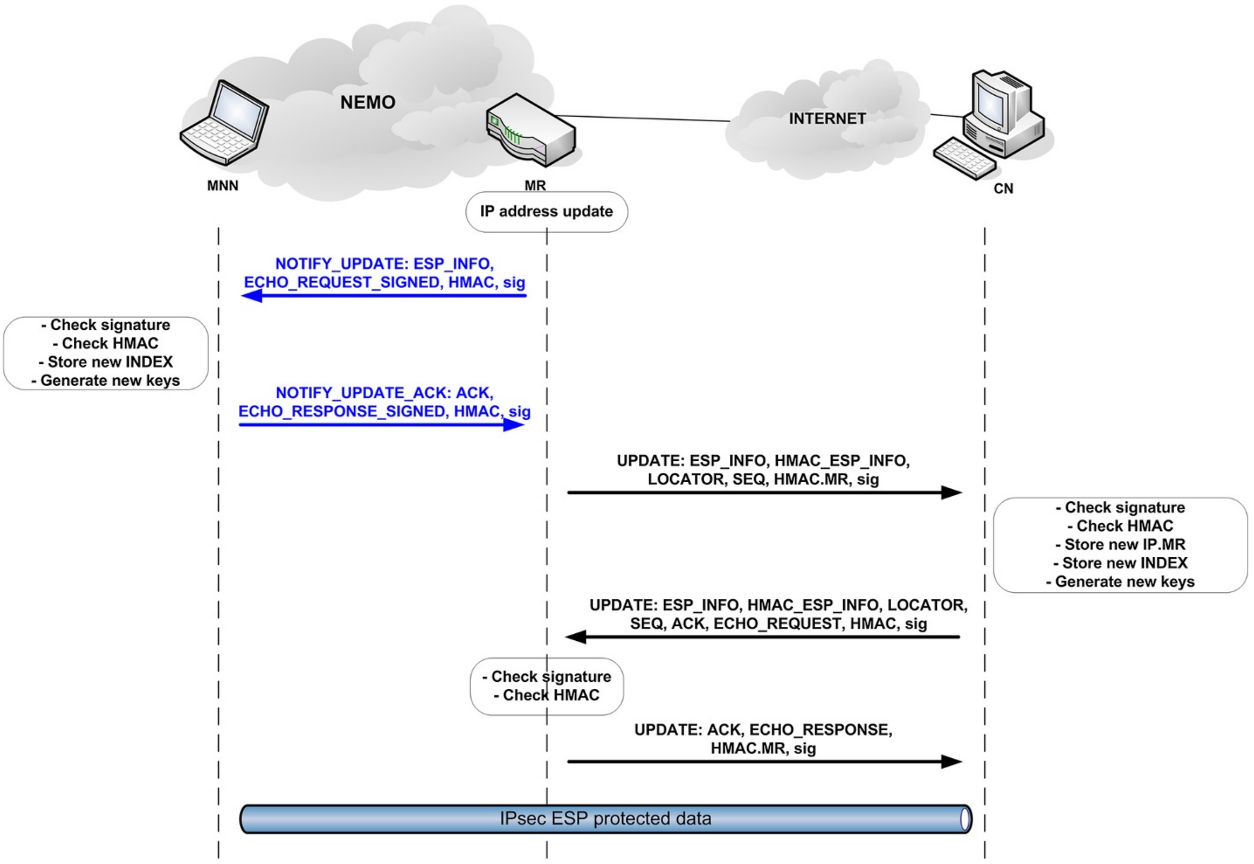

Figure 3 NeMHIP association update.

vulnerabilities of such an approach. To this end, in our network mobility management protocol, the MR is in charge of managing the mobility of the entire network and it is also in charge of agreeing the end-to-end keys on behalf of the MNNs when mobility events take place.

More specifically, and taking into account that NeMHIP has been developed based on the HIP protocol, its basic goal can be expressed as follows: the protocol must not introduce security vulnerabilities to the network mobility management compared to the HIP protocol. Two additional security goals have been defined.

- The protocol must provide end-to-end security properties for user data services. User data exchanges between the MNN and the CN should be provided with mutual authentication, confidentiality, and integrity protection.
- The protocol must avoid the security vulnerabilities of a delegation of signaling right approach, despite being the MR in charge of managing the mobility of the entire network.

Further details on the security features are out of the scope of this article.

Regarding the efficiency of the protocol, we have defined that the protocol must ensure the advantages of a delegation of signaling rights approach. That is, the signaling overhead should be reduced, the signaling path should be optimized and the manageability of the solution should be increased.

Table 3 Definition of the packets exchanged in a NeMHIP association update

Packet	Direction	Fields
$NOTIFY\_UPDATE$	$MR \rightarrow MNN$	$\{\{ESP_{INFO_{CN,MNN}}, N,$ $HMAC(K_{MR,MNN_i} \vert m\}_{K_{MR,MNN_e}}\}_{K^-_{MR}}$
$NOTIFY\_UPDATE_{ACK}$	$MNN \rightarrow MR$	$\{\{ESP_{INFO_{CN,MNN}}, ECHO(N), ACK,$ $HMAC(K_{MR,MNN_i} \vert m)\}_{K_{MR,MNN_e}}\}_{K^-_{MNN}}$
$UPDATE1$	$MR \rightarrow CN$	$\{LOCATOR, \{ESP_{INFO_{CN,MNN}}, SEQ,$ $HMAC(K_{MR,CN_i} \vert m)\}_{K_{MR,CN_e}}\}_{K^-_{MR}}$
$UPDATE2$	$CN \rightarrow MR$	$\{LOCATOR, \{ESP_{INFO_{CN,MNN}}, ACK, SEQ, N,$ $HMAC(K_{MR,CN_i} \vert m)\}_{K_{MR,CN_e}}\}_{K^-_{CN}}$
$UPDATE3$	$MR \rightarrow CN$	$\{ACK, \{ECHO(N),$ $HMAC(K_{MR,CN_i} \vert m)\}_{K_{MR,CN_e}}\}_{K^-_{MR}}$

Those considerations can be summarized stating that the security vulnerabilities of the delegation of signaling rights strategy should not be solved worsening the manageability and increasing the signalling overhead, but the advantages of delegating signaling rights have to be maintained. This way, efficiency and security can be provided simultaneously.

4 Analytical signaling cost evaluation

As mentioned, protocols and procedures to be introduced in the ITS context have to be efficient. Because of that, this section presents an analysis conducted over the NeMHIP protocol for evaluating its efficiency in terms of signaling cost under different conditions. Moreover, since wireless access links are used in a network mobility scenario, the amount of signaling transmitted over these links is considered a good parameter for evaluating the efficiency of the signaling protocol. We have defined a mathematical model to compute the signaling cost of NeMHIP, measured in bytes per time unit, and have compared it with the most complete network mobility management solution based on HIP built over the delegation of signaling rights paradigm, that is HIP-NEMO [4].

In general terms, the total signaling cost per unit time for a generic HIP-based network mobility protocol consists of Φ_{SA}, $\Phi_{UPDATE_{MR}}$, and $\Phi_{UPDATE_{MNN}}$, where Φ_{SA} is the total signaling cost per unit time of establishing the HIP associations; $\Phi_{UPDATE_{MR}}$ is the signaling cost per unit time of the network mobility management process when the MR changes its point of attachment; and $\Phi_{UPDATE_{MNN}}$ is the signaling cost per unit time generated by the MNN when it requests an update of its associations, commonly due to rekeying needs.

4.1 Model assumptions

The overall signaling cost generated in a cell per unit time is computed under the assumption that all the incoming requests are served, that is, we assume that the cell is not overloaded. In addition, we assume that there is an equilibrium between the arrivals and departures of mobile networks in the cell. In fact, we denote the number of mobile networks in the cell by M, while the number of MNNs per mobile network is represented by N_{MNN}.

To model the time a mobile network remains in a cell, we assume that the cell residence time is an exponentially distributed variable with mean value $1/\eta_{MR}$. Moreover, to compute the cell crossing rate, we use the City Section Model (CSM) [13] as the mobility model because it is a demanding model compared to other models such as the train mobility model.

Whenever an application running on a CN requests communication with an MNN with whom no previous association exists, establishment of a NeMHIP association is initiated. To model this connection query arrival process for each MNN, we assume a Poisson process with average session arrival rate represented by λ_{SA}. We assume that the duration of an established NeMHIP association is also an exponentially distributed variable, with mean value $1/\mu_d$.

MNNs can also themselves initiate requests for updating NeMHIP associations. Since these requests are typically related to rekeying necessities, they can be triggered according to the length of the keys, their usage time, the security needs of the application, the trust level of the peer, etc. Consequently, we assume that the requests by MNNs for updating associations follow a Poisson process. Therefore, the time elapsed between two consecutive NeMHIP association updates requested by a single MNN is an exponentially distributed variable with mean value $1/\eta_{MNN}$.

Figure 4 illustrates the timing diagram considered in this study.

4.2 Analytical model description

When a certain mobile network enters a cell, all the previously established NeMHIP associations must be updated. At the same time, new NeMHIP association requests can be initiated during the cell residence time of the mobile network. Therefore, following the equilibrium assumption between arrivals and departures in the cell, the average number of *subsessions*, defined as a part of a session within the same cell, is computed as the sum of

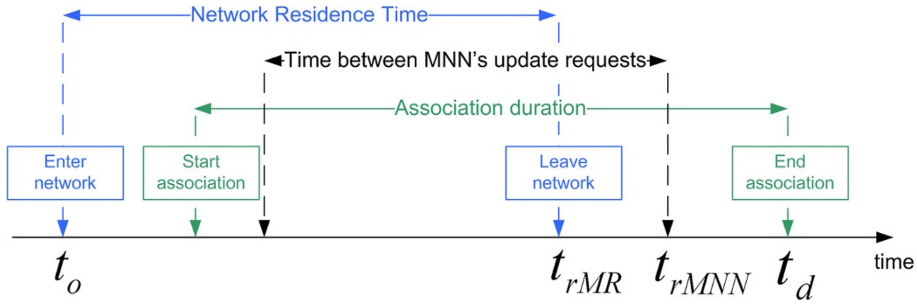

Figure 4 Timing diagram.

the average number of NeMHIP associations handed over and the number of new NeMHIP associations generated, $N_{MNN}M\lambda_{SA}$:

$$\lambda_{HO} = \frac{\eta_{MR}}{\mu_d} N_{MNN}M\lambda_{SA} \quad (1)$$

MNNs can also at their own initiative request that the established NeMHIP associations be updated. As previously mentioned, these requests can result from rekeying needs dependent on various issues. The expression for modeling this behavior is given by the following formula, where the average number of NeMHIP association update requests sent by the MNNs is computed as

$$\lambda_{MNN_{update}} = \frac{\eta_{MNN}}{\mu_d} N_{MNN}M\lambda_{SA} \quad (2)$$

In the same way, the average number of mobile network handovers is computed as

$$\lambda_{HO_{NEMO}} = \frac{\eta_{MR}}{\mu_d} M\lambda_{SA} \quad (3)$$

Using the expressions given above, we now show the formulas for computing the different contributors to the total signaling cost per unit time over the wireless link

$$\Phi_{SA} = (S_{I1'} + S_{R1'} + S_{I2'} + S_{R2''})N_{MNN}M\lambda_{SA} \quad (4)$$

$$\Phi_{UPDATE_{MR-CN}} = (S_{U1} + S_{U2} + S_{U3})\lambda_{HO} \quad (5)$$

$$\Phi_{UPDATE_{MNN}} = (S_{U1} + S_{U2} + S_{U3})\lambda_{MNN_{update}} \quad (6)$$

where S_x denotes the size in Bytes of the various exchanged packets, and x denotes the packet type.

When a mobile network changes its point of attachment, apart from updating all the established NeMHIP associations, its location must also be updated in the RVS. This update takes place regardless of whether there are established associations. Since the session arrival process follows a Poisson distribution, the probability of having k sessions in the mobile network when a handover takes place is obtained using the following equation:

$$P_{r_k} = \frac{(\frac{N_{MNN}\lambda_{SA}}{\mu_d})^k}{k!} e^{-(\frac{N_{MNN}\lambda_{SA}}{\mu_d})} \quad (7)$$

Therefore, since the MR updates its location in the RVS even if no NeMHIP associations have been established ($k = 0$), the signaling cost per unit time generated by the update of the location in the RVS by the MR is expressed as

$$\Phi_{UPDATE_{MR-RVS}} = (S_{U1} + S_{U2} + S_{U3})\lambda_{HO_{NEMO}} e^{-(\frac{N_{MNN}\lambda_{SA}}{\mu_d})} \quad (8)$$

Now, the total signaling cost per unit time over the wireless access link is defined as

$$\Phi_{NEMO} = \Phi_{UPDATE_{MR-RVS}} + \Phi_{SA} + \Phi_{UPDATE_{MR-CN}} + \Phi_{UPDATE_{MNN}} \quad (9)$$

The analytical model for HIP–NEMO is the same as that obtained for NeMHIP, but the packet sizes of the HIP–NEMO association establishment vary.

4.3 Analytical results

In computing the results we considered the following parameters: $r_{NEMO_{access}} = 500$ m, to model a realistic coverage area of IEEE 802.11 technology. In the evaluation we assumed that the mobile network moves at a maximum speed of 110 km/h and a minimum of 20 km/h, and thus, following the CSM mobility model, with the given cell radius, the mobile network hands over every 4.722 min. Furthermore, we assumed that there were 50 mobile networks on average in the cell, $M = 50$. To define NeMHIP packet sizes, we assumed that mandatory cryptographic suites were implemented in the nodes. Therefore, packet sizes were as follows (Bytes): $S_{I1'} = 80$, $S_{R1'} = 1300$, $S_{I2'} = 1704$, $S_{R2'} = 224$, $S_{R2''} = 288$, $S_{U1} = 184$, $S_{U2} = 84$, $S_{U3} = 88$, $S_{NOTIFY_{UPDATE}} = 1152$, and $S_{NOTIFY_{UPDATE_{ACK}}} = 1056$.

Figure 5 shows a comparison of the signaling cost per unit time for the NeMHIP and HIP–NEMO protocols for different association request mean values, λ_{SA}, and different numbers of MNNs in the mobile network. To compute this signaling cost and analyze how both protocols operate under the same parameter configuration, we assumed that the association update request rate for MNNs was the same for both protocols. In this study, we considered that the mean duration of a communication is 2 min, which models a typical conversational communication, i.e., $\mu_d = 1/120s^{-1}$.

As expected, the higher the session arrival rate is, the higher is the signaling cost over the wireless link. On the other hand, as can be seen in Figure 5, the signaling costs generated by the NeMHIP and HIP–NEMO protocols differ by 8.7% with $\lambda_{SA} = 0.01$, which is considered an unusual and pessimistic scenario with respect to the association request rate. Nevertheless, this increase in the signalling cost is considered to be negligible.

Next, we investigated the impact of the rekeying rate requested by the MNN in the signaling cost over the wireless link. In this case, as the HIP–NEMO protocol does not solve the situation where rekeying coincides with mobility, i.e., the MR is not in charge of rekeying the end-to-end association when a mobility event takes place, we assume that in the HIP–NEMO protocol the MNNs request rekeying at their own initiative with a higher

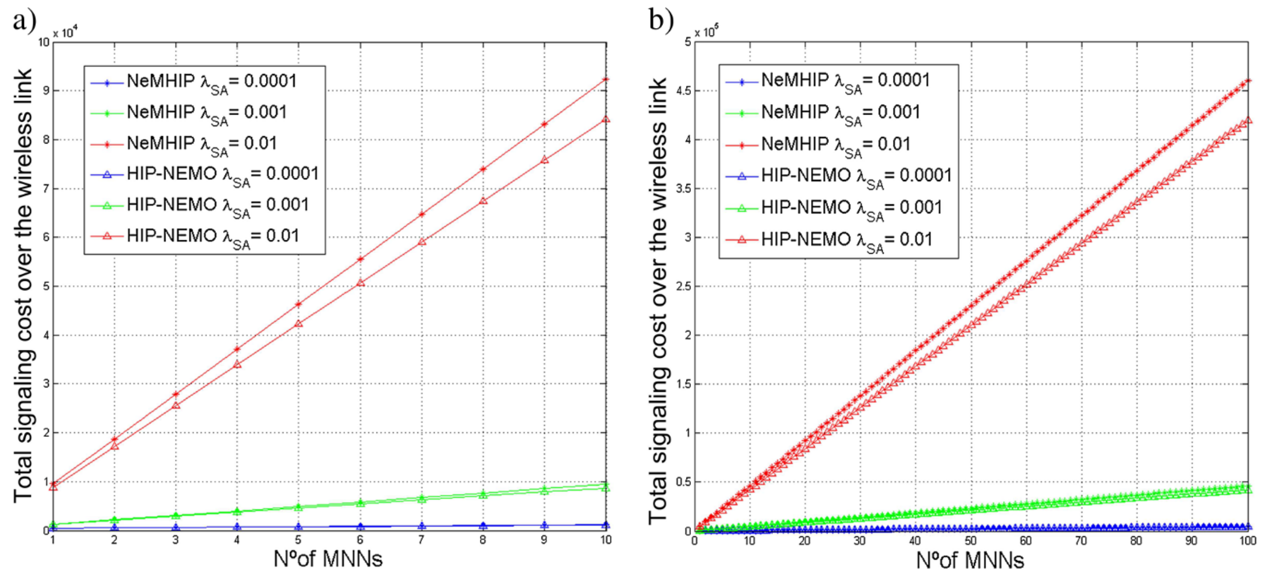

Figure 5 Signaling cost over the wireless access link. (a) Up to 10 MNNs onboard. **(b)** Up to 100 MNNs onboard.

frequency than in the NeMHIP protocol. This procedure is assumed because the policy of rekeying should be rapid enough to prevent vulnerabilities related to mobility events. The rationale behind this assumption is that MNNs are oblivious to mobility. By assuming this behavior, we can evaluate the performance of both protocols on equal terms with respect to security support.

To study this scenario, we considered the following cases with respect to the rate of update requests by MNNs.

- Case (1): $\eta_{MNN_{NeMHIP}} = 1/600$ and $\eta_{MNN_{HIP-NEMO}} = 1/120$. This case models the scenario where MNNs in the NeMHIP protocol request rekeying the end-to-end NeMHIP association every 10 min, while the MNNs in the HIP–NEMO protocol do so every 2 min.
- Case (2): $\eta_{MNN_{NeMHIP}} = 1/1800$ and $\eta_{MNN_{HIP-NEMO}} = 1/360$. This case models the scenario where the MNNs in the NeMHIP protocol request rekeying every 30 min, while those in the HIP–NEMO protocol do so every 10 min.
- Case (3): $\eta_{MNN_{NeMHIP}} = 1/2400$ and $\eta_{MNN_{HIP-NEMO}} = 1/720$. This case models the scenario where the MNNs in the NeMHIP protocol request rekeying the association every 40 min, while those in the HIP–NEMO protocol do so every 12 min.

The values for the rekeying rates were selected based on the mobile network handover rate (every 4.722 min), which for the case of NeMHIP ensures that end-to-end keys are renewed with that rate, while for the HIP–NEMO protocol MNNs should request renewing the keys on their own initiative to protect communications. In addition, the duration of the communication was considered, for which we assumed two cases: (1) the mean duration is 2 min ($\mu_d = 1/120s^{-1}$), which as mentioned before, models a typical conversational communication; and (2) the mean duration is 80 min ($\mu_d = 1/4800s^{-1}$), which models a file download.

As mentioned before, in the HIP–NEMO protocol, the end-to-end associations are not rekeyed with the handovers of the mobile network, and thus, MNNs have to request rekeying at their own initiative. As a result, we assumed that the rekeying rates of MNNs for HIP–NEMO should at least be the same of the duration of the shortest communication (case 1), so that it is secured, and in all the cases higher than the rekeying rate of NeMHIP (cases 2 and 3), to mitigate vulnerabilities related to mobility events. It should be pointed out that although we have assumed a higher update frequency of MNNs in the HIP–NEMO protocol, the end-to-end NeMHIP associations are rekeyed more often compared with those of the HIP–NEMO protocol owing to the cell crossing rate of the mobile network. To compute the signaling costs $\lambda_{SA} = 0.01$ was assumed. Figure 6 shows the obtained results.

As can be seen in Figure 6, the signaling cost generated by the HIP–NEMO solution is higher than that generated by the NeMHIP solution. The difference between the costs generated by these protocols increases from 2.1 to 16.61% with the increase of the rekeying rates. In the same way, the difference between the costs generated by the protocols is higher, varying from 45.67 to 73.47%, when the mean duration of the communication (μ_d) is longer. This is because the number of subsessions in a cell depends on the mean duration of the communication, and thus, on the

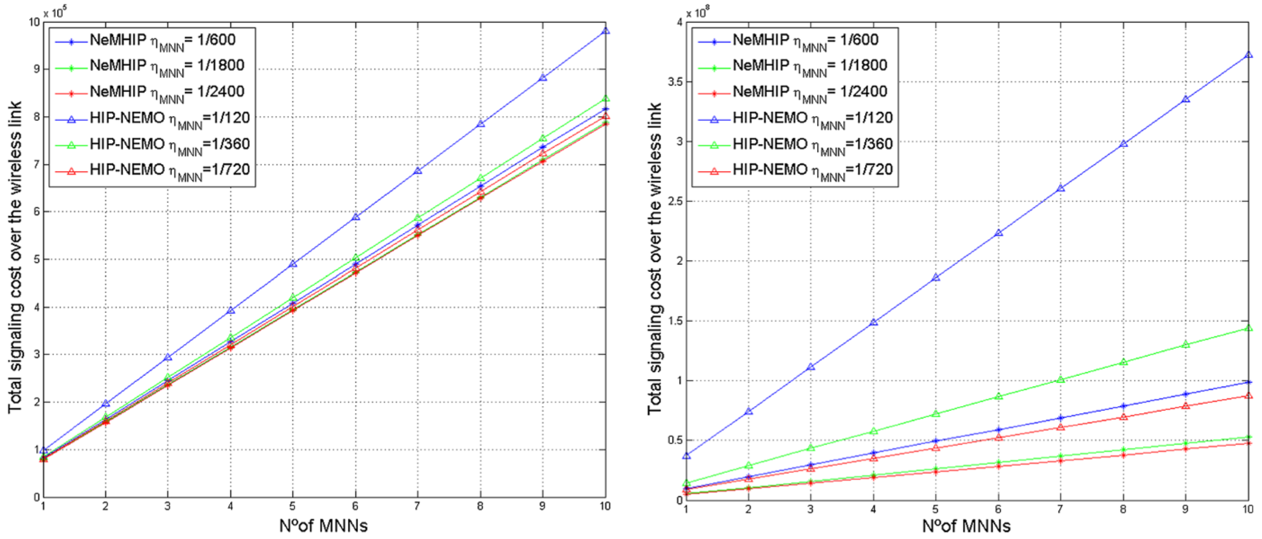

Figure 6 Signaling cost over the wireless access link for different MNN rekeying rates.

number of associations that have to be rekeyed. Therefore, the NeMHIP protocol outperforms the HIP–NEMO protocol in terms of signaling cost over the wireless link.

We also investigated the difference between signaling costs of the NeMHIP and HIP–NEMO protocols when a mobility event takes place and the MNNs happen to request rekeying at the same precise instant. For doing so, we considered a scenario where up to 100 MNNs have an association established with up to 100 CNs.

Figure 7 shows that the signaling cost generated by the HIP–NEMO protocol is 50% higher than that of the NeMHIP protocol. This increase in signaling cost is the result of the additional end-to-end updates required for rekeying the communication between the MNN and the CN to avoid packet discards due to the ESP anti-replay protection. These end-to-end updates are not required in the NeMHIP protocol.

It is interesting to point out that owing to the issues that imply rekeying the end-to-end associations, a Poisson process was assumed to model the rekeying requests of the MNNs. Depending on local policies, these requests could be sent periodically and the process could be modeled by a constant timer. Nevertheless, obtained results would likely be very similar for both models.

In our study, we assumed a stationary situation, where the mobile network arrivals and departures equal, and so, the number of mobile networks in a cell remains constant. To analyze the signaling cost for a varying number of mobile networks, a study in the time domain should be conducted. In addition, our model assumes that the cell is not overloaded, which results in serving all the incoming requests, i.e., exchanging all the required signaling to assure the correct performance of the communications. A study on a loaded cell would provide insight in the impact of the signaling cost in the overall traffic, and on the required prioritization policies. These aspects have to be aligned with the specification of the number of onboard nodes, number of mobile networks in the cell during a certain period of time, generated traffic by each onboard node, wireless access technology characteristics, and so on, that will be covered in our future works.

On the other hand, the study relies on the CSM mobility model, which is focused on the behavior of vehicles in a grid of streets, so the considered velocities are tight to such scenario. Since the selected mobility model governs the handover rate, changes in the model would vary the results. As a consequence of this, in our future works we plan to study the performance of the NeMHIP protocol in other ITS contexts, such as motorways or high-speed trains.

From the obtained results, we can conclude that when both protocols implement the same security level, the NeMHIP protocol is more efficient than the HIP–NEMO protocol in terms of signaling cost owing to the integration of the security and mobility management frameworks. Consequently, allowing the MR to be in charge of updating the end-to-end keys whenever a mobility event occurs, while ensuring end-to-end confidentiality and integrity, results in an efficient solution for managing mobility securely.

5 Conclusions

One of the main requirements that Information and Communication Technologies should satisfy to be introduced in the ITS context is efficiency. In fact, introducing efficient and lightweight protocols will make easier the

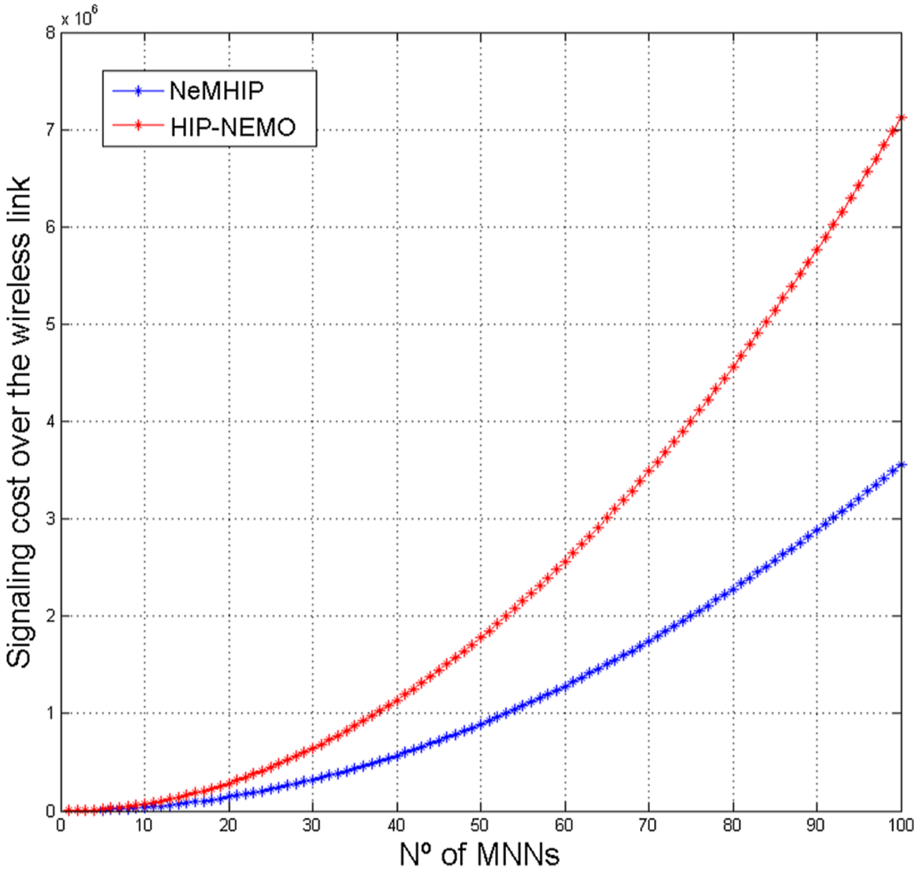

Figure 7 Signaling cost over the wireless access link when a mobility event takes place. (a) Connection duration = 2 min. **(b)** Connection duration = 80 min.

fulfilment of the high performance requirements such as the timeliness of messages, which is a critical parameter in safety-oriented applications, and the satisfaction of end user service quality expectations. Owing to these aspects, the introduction of efficient solutions in the ITS context leads to a successful deployment and penetration of ITS technologies. Another important concern in the ITS context is the provision of secure communications. Protecting vehicle-to-infrastructure communications will mitigate attacks that may affect the operation of the vehicle, and consequently, will increase human safety. Therefore, efficiency and security are critical issues that have to be addressed by any solution to be successfully introduced in the ITS context.

A vehicle in an ITS context is equipped with several onboard nodes that demand connectivity to the outside network. Therefore, from a communications point of view, a vehicle can be regarded as a mobile network whose mobility has to be managed by means of network mobility management protocols. This network mobility management procedure should be efficient in terms of signaling cost so as not to overload the wireless links used in mobility scenarios such as in an ITS context. In addition, it should not introduce security leaks or render security measures useless.

Although the MIPv6-based NEMO BS protocol has been adopted by standardization bodies, it has drawbacks, such as suboptimal routing or an inadequate security level, which must be overcome. As a result, alternative protocols are also being considered for use in network mobility contexts. The most complete protocol covering these contexts is the HIP, thanks to the security properties and optimal routing it provides. In fact, solutions that consider HIP as the base protocol have already been defined for addressing network mobility contexts [4-6]. These solutions are based on the concept of delegation of signaling rights. That is, the established end-to-end SAs are managed by a delegate, resulting in a known security vulnerability. To the best of the authors' knowledge, no solution that simultaneously ensures both efficiency and security support has been released for managing network mobility in ITS scenarios.

In this article, we have presented the NeMHIP protocol, an efficient and secure HIP-based network mobility management protocol. NeMHIP guarantees an adequate level of security to the end-to-end data exchanges between nodes communicating to each other, as well as to signaling message exchanges. At the same time, despite the introduction of this security framework, NeMHIP constitutes an efficient solution in terms of signaling cost over the wireless link, thanks to the approach of letting the MR be in charge of managing the end-to-end SAs and the mobility management at the same time. Despite NeMHIP is not based on the delegation of signaling rights concept, the manageability level is not penalized compared to the solutions that are built over this concept.

Moreover, we evaluated the efficiency in terms of signaling cost of the NeMHIP protocol through analytical modeling, and verified that, with respect to signaling on equal terms of security support, NeMHIP is more efficient than HIP–NEMO [4], hitherto the most complete solution that makes use of delegation of signaling rights. Therefore, we can confirm that the manageability level of an approach based on delegation of signaling rights is not only maintained, but also in fact it is enhanced.

In conclusion, the NeMHIP protocol is a secure network mobility management solution, because it avoids the vulnerabilities of the delegation of signaling rights paradigm, and it ensures confidentiality and integrity protection for end-to-end data. Regarding efficiency, the signaling cost of NeMHIP transmitted over a wireless link is comparable to and even better in certain scenarios, than that of a network mobility management solution using delegation of signaling rights, and thus, NeMHIP is a suitable solution for the ITS context. The NeMHIP protocol is to the best of the authors' knowledge, the only efficient solution that also guarantees security for managing network mobility in ITS scenarios.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

The study was produced within the Training and Research Unit UFI11/16 funded by the UPV/EHU.

Author details

[1]Department of Communication Engineering, University of The Basque Country, Alameda Urquijo s/n, 48013 Bilbao, Spain. [2]RSM Department, TELECOM Bretagne, Institut Mines Télécom / Télécom Bretagne, IRISA / D2 / OCIF, 35510 Cesson-Sevigne, France.

Received: 18 April 2012 Accepted: 24 October 2012
Published: 14 November 2012

References

1. R Baldessari, A Festag, M Lenardi, C2C-C consortium requirements for usage of NEMO in VANETs, IETF draft, draft-baldessari-c2ccc-nemo-req-00, 2000, http://tools.ietf.org/html/draft-baldessari-c2ccc-nemo-req-01
2. V Devarapalli, R Wakikawa, A Petrescu, P Thubert, Network mobility (NEMO) basic support protocol, RFC 3963, 2005, http://tools.ietf.org/html/rfc3963
3. P Nikander, A Gurtov, T Henderson, Host identity protocol (HIP): connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks. IEEE Commun. Surv. Tutor. **12**(2), 186–204 (2010)
4. S Nováczki, L Bokor, G Jeney, S Imre, Design and evaluation of a novel hip-based network mobility protocol. J. Netw. **3**(1), 10–24 (2008)
5. J Melen, J Yitalo, P Samela, T Henderson, Host identity protocol-based mobile router (HIPMR), IETF draft, draft-melen-hip-mr-02, 2009, http://tools.ietf.org/html/draft-melen-hip-mr-02
6. J Ylitalo, J Melén, P Salmela, H Petander, in *WWIC'08: Proceedings of the 6th international conference on Wired/wireless internet communications*. An experimental evaluation of a hip-based network mobility scheme. Tampere, Finland, May 2008. Lecture Notes in Computer Science, vol. 5031 (Springer-Verlag Berlin, Heidelberg, 2008), pp. 139–151
7. P Nikander, J Arkko, in *SPW'02: Security Protocols Workshop*, ed. by B Christianson, B Crispo, JA Malcolm, and M Roe. Delegation of signaling rights. Cambridge, UK, April 2002. Lecture Notes in Computer Science, vol. 2845 (Springer Berlin Heidelberg, 2004), pp. 203–214
8. P Jokela, R Moskowitz, J Melen, Using the encapsulating security payload (ESP) transport format with the host identity protocol (HIP), IETF draft, draft-jokela-hip-rfc5202-bis-02, 2012, http://tools.ietf.org/html/draft-jokela-hip-rfc5202-bis-02
9. T Henderson, C Vogt, J Arkko, Host mobility with the host identity protocol, draft-ietf-hip-rfc5206-bis-03, IETF draft, 2011, http://tools.ietf.org/html/draft-ietf-hip-rfc5206-bis-03
10. N Toledo, JM Bonnin, M Higuero, E Jacob, in *Proceedings of IEEE CCNC'11: Consumer Communications and Networking Conference,* Las Vegas, USA. Fundamentals of NeMHIP: an enhanced HIP based NEMO protocol (IEEE Press Piscataway, NJ, USA, 2011), pp. 1132–1133
11. N Toledo, JM Bonnin, M Higuero, Performance evaluation of user applications in the ITS scenario: an analytical assessment of the NeMHIP protocol. J. Netw. Comput. Appl. (Special Issue on Vehicular Communications and Applications) (2012). doi:10.1016/j.jnca.2012.02.005
12. N Toledo, M Higuero, E Jacob, J Matias, Analytical evaluation of a HIP registration enhancement for NEMO scenarios. IEEE Commun. Lett. **15**(5), 587–589 (2011)
13. MS Hossain, M Atiquzzaman, in *Proceedings of GLOBECOM'09: The 28th IEEE conference on Global telecommunications,* Honolulu, Hawaii, USA. Stochastic properties and application of city section mobility model (IEEE Press Piscataway, NJ, USA, 2009), pp. 1140–1145

doi:10.1186/1687-1499-2012-339
Cite this article as: Toledo *et al.*: Analytical efficiency evaluation of a network mobility protocol for Intelligent Transportation Systems. *EURASIP Journal on Wireless Communications and Networking* 2012 **2012**:339.