SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2010; **3**:114–129
Published online 1 September 2009 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.134

Performance analysis of secure on-demand services for wireless vehicular networks

Etienne S. Coronado*, † and Soumaya Cherkaoui*, †

Department of Electrical and Computer Engineering, Université de Sherbrooke, Quebec, Canada

Summary

Wireless vehicular communications pose significant challenges for the deployment of next generation roadside services. Some important issues that must be tackled are security, billing, and reliability while guarantying a scalable service delivery. This paper addresses the assignation of secure service session parameters upon the reception of on-demand service requests by an incumbent services district domain and studies and analyses the performance of the underlying mechanisms. Three types of service request protocols are introduced in our work defined as single-hop (SHI-RQ), extended connectivity (EC-RQ), and multi-hop (MHI-RQ) service requests. A detailed analytical model and cost study for the access protocols are presented. Our analysis study covers the estimation of total cost in terms of latency for each access protocol with different mobility characteristics and vehicle densities within the service coverage area and across different serving district domains. The analytical results are consistent with the experimental one and show that the access protocols cost in terms latency remains acceptable for a realistic number of serviced vehicles even at high speeds. Copyright © 2009 John Wiley & Sons, Ltd.

KEY WORDS: vehicular networks on-demand services; service provisioning; security; billing

1. Introduction

Vehicular *ad hoc* networks (VANETs) are networks that are enabled by short to medium-range communication systems for vehicle-to-vehicle (V2V) or vehicle-to-roadside (V2I) communications. The potential benefits associated to enabling road-safety applications through VANETs are well known. This type of applications includes real-time collision avoidance warnings as well as the exchange of driving parameters among vehicles for a safer driving. Besides these useful and sometimes vital functionalities, commercial non-safety related services are also envisioned to coexist with safety applications within the realm of future VANET and vehicular networks. The array of these commercial services can be broad, ranging from internet access, vehicle infotainment, navigation assistance to transportation logistics management, and high speed electronic toll collection (ETC).

Service oriented applications represent an interesting opportunity in terms of economic potential since different service providers can potentially supply useful applications on the roadside for both drivers and passengers through open standard platforms. In a

*Correspondence to: Etienne S. Coronado or Soumaya Cherkaoui, Department of Electrical and Computer Engineering, Université de Sherbrooke, Quebec, Canada.
†E-mail: etienne.coronado@usherbrooke.ca; or soumaya.cherkaoui@usherbrooke.ca

competitive market, providers will be distinguished by the type of added-value services and the type of service offerings to users. However, the capacity of viably enabling non-safety applications on the road will rely on the methods roadside services will be discovered, accessed and kept reliable through the wireless infrastructure. These factors are likely to determine how business models are offered on the road and how these solutions can be maintained scalable through different network domains. While safety applications will be open and free-access for all for the sake of general public safety, commercial applications will be open-access only for traveling vehicles that will be willing to pay some kind of fee. One main difference between safety and commercial applications is then the fact that a prospective service requester will be subjected to verification and billing procedures prior to retrieving access to a service. Some challenges might arise concerning the request of services by potential users given that the latter might not be attached to any sort of home network service infrastructure. Business models for non-safety service offerings on the road are, in fact, likely to be 'spontaneous' on-demand ones. Based on this premise, it is valid to assume that service providers will have poor or even no knowledge of transitory users whenever a service request is executed. Nevertheless, exchanges of information between transitory users and service providers must be kept reliable and secure, especially, when sensitive information is transferred such as financial information or disclosure of user identities. Therefore, adequate secure and billing mechanisms must be designed for vehicular. Figure 1 illustrates a general service provisioning scenario in a V2V and V2I communication modes.

Many undergoing efforts are targeted toward designing and developed specific communication protocols for V2V and V2I communications. In North America

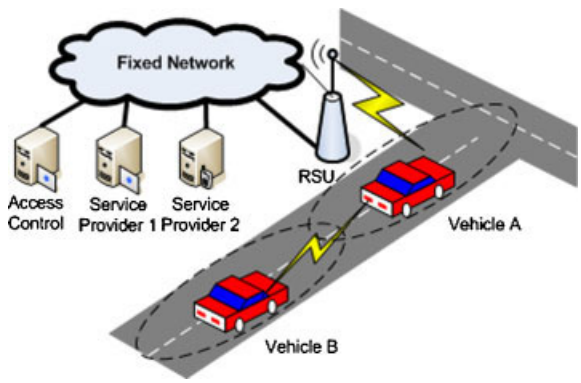

Fig. 1. Vehicular communication scenario.

the Intelligent Transport Systems (ITS) is working on the development of the 5.9 GHz Direct Short Range Communication (DSRC). For non-safety applications, the way roadside services are broadcasted in DSRC is defined in the IEEE 1609.3 [1] trial standard for Wireless Access in Vehicular Environments (WAVE). The information related to specific providers and corresponding channels is contained in a frame structure called WAVE Service Advertisement (WSA) which carries the Provider Service Table (PST). Before the Roadside Unit (RSU) announces the availability of services within its transmission range, the WSA is encapsulated in an extended frame called WAVE Service Information Element (WSIE). The WSIE frame is then received and processed by transitory users to retrieve the parameters that will be employed to request specific services. The process to allow provider applications to be registered at the WAVE management entity (WME) consists of disclosing information such as channel of operation, address information, description of the services being offered, and application priority. Once an application is successfully registered at the local PST, it is ready to be advertised through the roadside infrastructure. Identifiers are used in the form of Provider Service Identifier (PSID) which guarantees the uniqueness of services and a Provider Service Context (PSC). The latter contains supplementary information to the service and depends on the PSID. Based on the above process, the On-board Unit (OBU) installed within the vehicle can distinguish and choose specific services contained in the PST. The discovery mechanisms as described in WAVE can be complemented by a robust service architecture which would be capable of generating session parameters in an on-demand basis, as well as, the creation of accounting registers for transitory users. The envisioned architecture must guarantee secure mechanisms for the delivery of information in a reliable way for vehicular environments.

In Europe, an initiative called Cooperative Vehicle-Infrastructure Systems (CVIS) [2] is developing a unified technical solution to communicate vehicles and infrastructure by means of an open application framework. Among the CVIS software applications, it is considered the deployment of cooperative urban applications whose objective is to create cooperative systems for travel data collection, personalized travel information, and traffic management. Additionally, cooperative fleet and freight applications are expected to result in the optimization of delivery logistics, and an increase of safety and security features for commercial vehicles. Moreover, cooperative monitoring

DOI: 10.1002/sec

would be focused in enhancing traffic monitoring by the assistance of fixed roadside sensors and sensors installed on vehicles to provide real-time information about the vehicle movements and the current state of the road.

The aforementioned initiatives highlight the need to tackle different challenges concerning access and provisioning of on-demand services in such a highly transitory environment. A service architecture in such context must offer secure and scalable access to roadside services. In this paper we classify different access protocols based on the service architecture we proposed in Reference [3], which is intended to offer secure service provisioning for spontaneous on-demand service requests on the road. The architecture is based on the premise that vehicles may request services anytime, anywhere and without being attached to any sort of home network. We also analyze the performance of the signaling cost of the proposed protocols executed between the requester and the service district domains. The rest of this document is organized as follows. Section 2 covers the related work of existing approaches intended for vehicular environments. Section 3 gives a description of the elements comprising the service district domain architecture, followed by the message notations of the proposed access protocols. Section 4 covers the analytical model with expressions of the corresponding signaling costs, followed by the analysis of the mobility model and numerical results. Finally, conclusions and future work are discussed.

2. Related Work

We reviewed existing relevant approaches concerning authentication, dispatching of security attributes, and accounting mechanisms; where the latter can be related to the implementation of billing mechanisms suitable for VANETs. The previous aspects become essential where referring to service provisioning in vehicular environments.

2.1. Security Approaches

One of the first works intended for vehicular environments was presented by El Zarki *et al*. [4] where it is proposed the Driver *ad hoc* Networking Infrastructure (DAHNI) framework. The authors assume vehicular *ad hoc* networking with access to a fixed infrastructure and which is intended mainly for traffic management. Their contribution regarding security relies on the implementation of digital signatures based on RSA (Rivest Sharmir Algorithm) encryption. These digital signatures are issued along with timestamps and sequence numbers to provide authentication between two parties. For managing public keys, a PKI infrastructure is envisioned adding robustness to the system.

Raya and Hubaux [5,6] consider the deployment of an Electronic License Plate (EPL) as a unique identifier of the vehicle and which can be issued by a trusted authority. Regarding privacy, it is proposed the use of anonymous key pairs that change frequently according to the driving speed and can be preloaded into the vehicle Tamper Proof Device (TPD) by a certificate authority. Additionally, it is proposed the security architecture is composed by a Vehicular Public Key Infrastructure (VPKI), where a CA issues certified public/private key pairs to vehicles. Authors also consider a hardware device tamper proof (TPD) to keep keying materials. In the authentication procedure, the vehicle signs each message with its private key and attaches the corresponding public key certificate. Dötzer [7] addresses privacy issues on VANETs, specifically, he assumes the use of pseudonyms as identifiers which change frequently and that can be mapped to identities. The approach used to validate this scheme considers a trusted authority that is responsible for storing real identities and handles their mapping to pseudonyms. Within the vehicle, there is a tamper resistant device in the form of a smart card which stores the set of pseudonyms and credentials for accessing services.

An access control scheme for application services in VN is proposed by Moustafa *et al*. [8]. Here, the authors present an authentication and authorization scheme based on a Kerberos model. Once a user request is released, the Kerberos Server at the service provider site responds with a Ticket Grant Ticket (TGT). If succeeded, the user is eligible to be granted with a Ticket Grant Service (TGS), which manages authorization to access information services. Moreover, the authors proposed a Kerberos proxy allocated in the access point (AP or RSU) to save bandwidth resources. After this process is done, the user receives an IP address (IPv4) from a DHCP server and a public key certificate. With this certificate key the user will be able to authenticate other users through the generation of a pairwise master key (PMK) for mutual authentication. The salient limitation of this architecture resides in weakness of internet connectivity since it is considered IPv4 and there is no handover management that supports extensive mobility. Another major concern is the lack of an end-to-end delay assessment of the access process to deem its feasibility in the deployment of VN.

DOI: 10.1002/sec

2.2. Accounting Approaches

An accounting approach addressed to mobile *ad hoc* networks (MANET) at a routing level is presented by Mohan and Joiner [9]. This approach does not consider a fixed infrastructure for accounting and billing purposes; hence, it suggests the scenario where collaboration of mobile nodes is required. The authors propose a model based on a load-based routing approach to distinguish between forwarding and originating packets in the network. For route metrics, a load value associates the number of packets buffered per node, knowing the number of originated and forwarded packets. For forwarding, it combines a load base hybrid routing (LHR) and a zone routing protocol (ZRP). At this point, the node in a zone knows the topology of every neighboring node and maintains a load/hop distance table in its cache. The advantage of this scheme is that it stimulates the nodes by rewarding them for forwarding packets and charging them for originating packets and requesting services from other nodes.

Another approach is presented by Buttyan and Hubaux [10]. The main idea is that the node employs a currency called nuggets that is used to 'pay' if it originates a request. The intermediates nodes acquire nuggets from the sent packet and then forward the packet. One drawback is that the number of nuggets to reach the destination is ambiguous. An open issue in billing models for VN relies on the integration of robust billing mechanisms that can be implemented and operated seamless at the SP infrastructure and at the V2V network. This means, that the billing process performed on the accounting server at the SP site, shall also be aware of the forwarding transactions carried out by communicating vehicles. This scenario can be thought in terms of a billing hybrid scheme for VN.

3. Service District Domain Architecture

Before detailing the main access protocols involved in a service request in the proposed architecture, let us give an overview of the serving administrative service architecture that processes these requests. In the proposed service delivery model, we define a service district domain as a logical zone that is mapped to a geographical area where a set of services from different roadside providers are broadcasted by the wireless infrastructure. Figure 2 shows the elements that fall within the administrative domain control and that are in charge of processing and validating incoming requests from potential users. Given the fact that transitory vehicles are highly mobility and may have unpredictable trajectories, the service district domain may most likely not have prior knowledge of potential users. Therefore the district domain has to rely on specific mechanisms suitable for this kind of *ad hoc* service requests. In the following are presented the main elements of the architecture. In the reminder of the text, we will use the terms 'vehicle' and 'user' indistinctly. Also, although the terms OBU and RSU have been introduced earlier relatively to DSRC technology, we will use hereafter the same terms to designate on board unit and roadside units that allow a vehicle to have access to any other type of wireless technology that is available on the road.

Security module (SEC). This module is composed by a subset of modules designated as Governmental Authorities (GA) and Private Authorities (PA). The GA is considered to be part of an official transport authority which can identify, when necessary, the real identity of vehicles. In Reference [6], it is proposed that governmental authorities or car manufacturers be the entities responsible of dispatching cryptographic material to vehicles and this material will be preloaded in tamper-proof devices within the vehicles. Certified key pairs (public keys, private keys) provided by official authorities must allow secure communications between two vehicles or a vehicle and the roadside infrastructure, even if no previous communication between them has been set up. This premise is supported by the assumption of the existence of strict control and registration procedures applied by official transport authorities to all vehicles and roadside units as well. Authentication of the public key certificates disclosed by requesters relies on the validation of the non-revocation state (certainty) of those certificates through certificate revocation lists (CRL) [11]. This type of authentication is based on the certainty of the current requester's certificates and not on a user-id/password based authentication; hence, any vehicle on the road which discloses its public key certificate can be scrutinized on the CRL. In our architecture, we assume that disclosed public certificates include their digital signature; therefore, a verification process of digital signature takes place. The PA module, it is responsible for generating security attributes intended for specific service sessions. This session parameters can be considered as temporary and valid only for the duration of the session. After an authentication of public certificate at the GA level takes place and is successful, the PA is able to generate the corresponding shared session keys between the user and service provider. Additionally, the PA can create temporary identifiers or pseudonyms for

DOI: 10.1002/sec

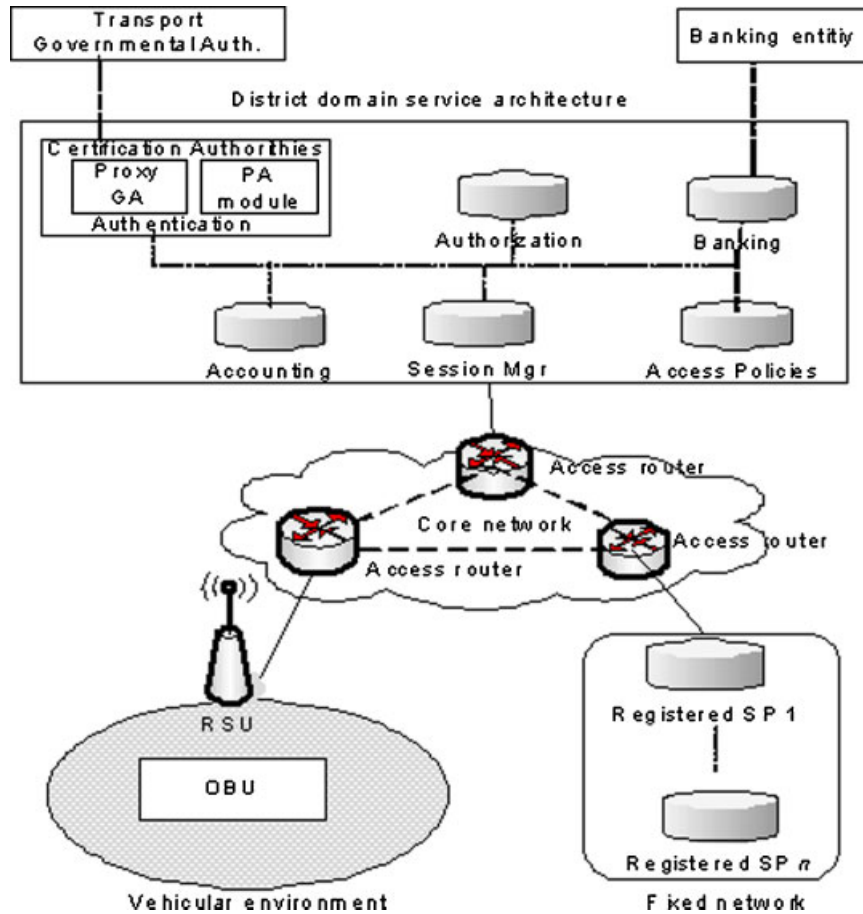

Fig. 2. Secure service architectural elements.

both the user and provider, respectively. Even though, this is an open architecture, the distribution of session parameters must be secured at all times to the corresponding recipients by encrypting the information with the user's public key in the case of the user and with a secret shared key between the provider and district domain.

Banking module (BNK). Depending on the services requested, the presence of banking entities may be required in order to ensure revenues for service providers. In general, any exchange of information related to the execution of financial transactions must be collected and analyzed at the BNK. Then, banking entities will be responsible for the issuance of on-demand credit units which will be the credentials that give the right to use specific services for a limited duration. We assume that there must be a pre-established relationship between the banking entity and the user for validation purposes that can be based either on some sort special banking credentials or identifier. This kind of banking validation resembles a credit-card payment or even a pre-paid card modality where the credit current balance of the potential user and its capacity to afford a specific service can be verified by an external banking entity or by a proxy module within the district service architecture. Notice that validation of the requester by the banking entity is performed after the authentication of communicating parties has been successfully completed. Once a successful validation of the user banking credentials takes place, the banking entity is able to dispatch the corresponding credit units and a transaction identifier that specifies the amount of content data to be retrieved or the maximum time duration for the service session.

Session manager (SM). The main function of the SM is to establish associations with other external SMs for the purpose of supporting scalability between multiple district domains. Any exchange of information between different district domains will be performed through the interaction of current participating SMs.

DOI: 10.1002/sec

This module is also responsible of creating a session ID and for collecting all the session parameters before forwarding the information to the RSU.

Accounting module. In this module temporary registers are created in order to keep track of transitory users. These registers record the dispatched session parameters of temporary users. The parameters include a temporary user identifier (pseudonym), a session identifier, credit units, timestamps, a transaction identifier, a provider identifier, a service identifier, and an expiration session time. Moreover, the accounting module contains specific policies which define the way temporary registers are maintained and updated.

Authorization module. This module grants resource assignation when validations at the previous modules have been completed.

Policy module. The execution of service policies defines the way how information is treated based on its labeled queuing priority and/or assigned bandwidth. These policies can be established when both users and providers agree to provide and accept a specific policy level.

We define three service request sub-protocols which are parsed and executed accordingly by the operating service district domain. These protocols take place depending on whether the OBU of the vehicle has a direct wireless connection to the RSU, is transiting through new district domains and needs its session information to be relayed, or needs a multi-hop connection though other OBU to reach the RSU. The exchange of these sub-protocol messages involves SM, SEC, and BNK. The transport protocol used by the messages is considered to be a reliable one such as TCP since the connection should be reliable to allow the exchange of service parameters. The service request sub-protocols are the following:

1. Single hop Initiation request protocol SHI-RQ. This set of messages is intended to initiate a service request in a single-hop vehicular to infrastructure mode.
2. Extension connectivity request protocol EC-RQ. This protocol is intended to provide continuous connectivity when a vehicle changes from one district domain to an adjacent one. Exchange of current session parameters takes place when performing handover operations between different service district domains.
3. Multi-hop Initiation request protocol MHI-RQ. This set of messages is intended to initiate a service request in a multi-hop environment.

We assume that the fixed infrastructure uses a trusted model which includes the RSU and service district domain architecture. In the following we express the message notation for the previous protocols.

3.1. Single-Hop Initiation Service Request Protocol [SHI-RQ] for On-Demand Services

A SHI-RQ message identifies a single-hop V2I on-demand service request which is executed by the OBU. First, the OBU sends an initial message to the RSU notifying its presence. Then, the RSU can reply to the message by requesting the OBU's public key certificates and intended service identifier. We assume that the initial exchange of SHI-RQ messages is part of the service discovery mechanism. The enlisted message notation the *SHI_RQ* protocol is illustrated in Figure 3 and the definition of acronyms is given in Table I.

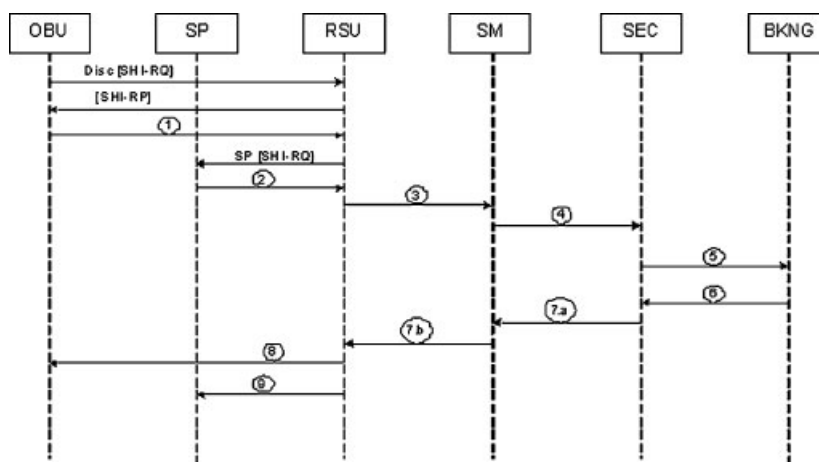

Fig. 3. SHI-RQ exchange messages.

DOI: 10.1002/sec

Table I. Service session symbols.

Symbol	Definition
PID1	User pseudonym
PID2	Provider pseudonym
Kss	Session key
Cert_{RSU}	RSU public certificate
Cert_{OBU}	User public certificate
Crd_unt	Credit bonus unit
$K_{\text{pa-sp}}$	Shared key authority-provider
K_{user}	User public key
Ss_id	Session ID
Srv_id	Service ID
Trn_id	Transaction identifier
T	Timestamp
Cert_{SP}	Service provider certificate
Bnk_id	Banking credential
Seq_{OBU}	User sequence number
Seq_{SP}	SP sequence number
Dist_id	District identifier

(1) Once service discovery is completed, the OBU sends an extended request message which includes the service ID that identifies the service the user is willing to acquire; public certificate which includes a digital signature; an encrypted banking credential and sequence number. Recall that there must be a pre-established relation between the prospective user and the banking entity for charging purposes.

$$\text{OBU} \rightarrow \text{RSU}: \text{Cert}_{\text{OBU}}, \text{Srv\_id}, \text{Enc}\{\text{Bnk\_id}\}_{K_{\text{bnk-obu}}}, \text{Seq}_{\text{OBU}}$$

(2) When the SHI-RQ is received at the RSU containing a specific service ID, the RSU sends a request message to the service provider (SP) for initialization purposes denoted as SP[SHI-RQ]. Then, the service provider replies with its public certificate and sequence number.

$$\text{SP} \rightarrow \text{RSU}: \text{Cert}_{\text{SP}}, \text{Seq}_{\text{SP}}$$

(3) The RSU parses and collects the information retrieved from the OBU and SP, respectively; and relays the service request message to the SM that resides at the service district domain.

$$\text{RSU} \rightarrow \text{SM}: \text{Cert}_{\text{SP}}, \text{Cert}_{\text{OBU}}, \text{Srv\_id}, \text{Enc}\{\text{Bnk\_id}\}_{K_{\text{bnk-obu}}}, \text{Seq}_{\text{OBU}}, \text{Seq}_{\text{SP}}$$

(4) The SM issues a session identifier which will serve as index for the whole validation process at the service district domain for either a successful or a failed attempt during the subsequent validation steps. A relayed message is sent to the SEC module which contains the public key certificates for both the user and SP. Digital signatures are then verified and public certificates are checked for their revoked status based on the most recent CRL.

$$\text{SM} \rightarrow \text{SEC}: \text{Cert}_{\text{SP}}, \text{Cert}_{\text{OBU}}, \text{SS\_id}, \text{Srv\_id}, \text{Enc}\{\text{Bnk\_id}\}_{K_{\text{bnk-obu}}}, \text{Seq}_{\text{OBU}}, \text{Seq}_{\text{SP}}$$

(5) The SEC module relays user banking parameters for their validation to the banking entity. There must be an association between the user public certificate and the corresponding shared secret key at the BNK; as a result, the BNK can identify the appropriate user record and charge the user accordingly to the service requested. If the validation of the user's credit is successful, a limited credit unit (credential) is generated for the specific use of the service; otherwise, the validation process is aborted.

$$\text{SEC} \rightarrow \text{BNK}: \text{Cert}_{\text{OBU}}, \text{SS\_id}, \text{Srv\_id}, \text{Enc}\{\text{Bnk\_id}\}_{K_{\text{bnk-obu}}}, \text{Seq}_{\text{OBU}}$$

(6) After the BNK verifies the credit of the potential user for that specific session, if successful, the BNK sends back to the SEC module a message including a transaction identifier, timestamp, and the encrypted credit unit by using the shared secret key between the user and the BNK.

$$\text{BNK} \rightarrow \text{SEC}: \text{SS\_id}, \text{Srv\_id}, \text{Enc}\{\text{Crd\_unt}\}_{K_{\text{bnk-obu}}}, \text{Trn\_id}, \text{T}, \text{Seq}_{\text{OBU}}$$

(7) Upon reception of a satisfactory message, the SEC is capable of generating the serving session key for the user and provider, as well as, the temporary user and provider ID (pseudonyms), respectively. The information intended for the provider is encrypted with a shared secret key between the registered provider and the district domain. The protected session parameters for the user include session ID, encrypted temporary user ID, session key, encrypted credit unit, transaction ID, sequence number, and district identifier. All session parameters for the user are encrypted by using its public key. The composed message is sent back to the RSU *via* the SM which acknowledges the validity

DOI: 10.1002/sec

of the session.

$$\text{SEC} \rightarrow {}_{a}\text{SM}(1) \rightarrow_{b} \text{RSU} : \text{Enc}\{\text{PID}_1,\ \text{SS\_id},\ \text{Dist\_id},\ \text{Kss},\ \text{Enc}\{\text{Crd\_unt}\}_{K_{\text{bnk-obu}}},\ \text{Trn\_id},\ \text{T},\ \text{Seq}_{\text{OBU}}\}_{K_{\text{OBU}}}$$

Now, the protected session parameters for the provider comprise the session ID, temporary SP ID, session key, transaction id, timestamp, and sequence number.

$$\text{SEC} \rightarrow {}_{a}\text{SM}(2) \rightarrow_{b} \text{RSU} : \text{Enc}\{\text{PID}_2,\ \text{SS\_id},\ \text{Kss},\ \text{Trn\_id},\ \text{T},\ \text{Seq}_{\text{SP}}\}_{K_{\text{SP}}}$$

(8) The relayed composed session parameters intended for the user within the wireless environment is appended to the RSU public certificate.

$$\text{RSU} \rightarrow \text{OBU} : \text{Enc}\{\text{PID}_1,\ \text{SS\_id},\ \text{Dist\_id},\ \text{Kss},\ \text{Enc}\{\text{Crd\_unt}\}_{K_{\text{bnk-obu}}},\ \text{Trn\_id},\ \text{T},\ \text{Seq}_{\text{OBU}}\}_{K_{\text{OBU}}},\ \text{Cert}_{\text{RSU}}$$

(9) The relayed composed session parameters intended for the provider is appended to the RSU public certificate.

$$\text{RSU} \rightarrow \text{SP} : \text{Enc}\{\text{PID}_2, \text{SS\_id}, \text{Kss}, \text{Trn\_id}, \text{T}, Seq_{\text{SP}}\}_{K_{\text{SP}}},\ \text{Cert}_{\text{RSU}}$$

3.2. Extension Connectivity Request Protocol [EC-RQ]

In order to provide a scalable solution, the exchange of control messages between adjacent service domains is required to let information of active service parameters be shared among operating SMs. For this reason, interconnection mechanisms need to be established on a logical level between neighboring district domains. In particular, it is necessary that two concurrent district domains maintain an active session alive without the need for the user to be registered in a new session at the new district domain.

(1) An EC-RQ message refers to the extension of service connectivity request upon the discovery of a new district domain (see Figure 4). For this case, the OBU sends an initial EC-RQ message

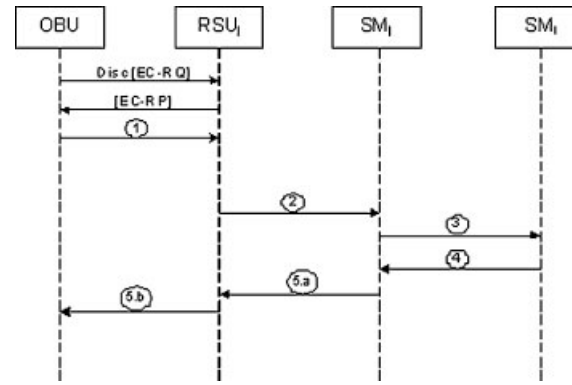

Fig. 4. EC-RQ exchange messages.

to the new discovered RSU_j. Then, the recently discovered RSU_j can reply by asking the OBU its current incumbent district identifier and session ID. Because the EC-RQ is a petition of connectivity for an existing session, RSU_j replies with its public key certificate, so the OBU can encrypt its disclosed parameters with the RSU_j's public key. The OBU sends an encrypted message which includes the current session identifier, temporary user identifier, transaction id, public certificate, district identifier, and sequence number.

$$\text{OBU} \rightarrow \text{RSU}_\text{j} : \text{Enc}\{\text{Cert}_{\text{OBU}},\ \text{SS\_id},\ \text{PID}_1,\ \text{Trn\_id},\ \text{Dist\_id},\ \text{Seq}_{\text{OBU}}\}_{K_{\text{RSU}_\text{j}}}$$

(2) Once this encrypted message is received at RSU_j, the latter sends an EC-RQ request message to SM_j to initiate a connectivity session identifier for the prospective session.

$$\text{RSU}_\text{j} \rightarrow \text{SM}_\text{j} : \text{Cert}_{\text{OBU}},\ \text{SS\_id},\ \text{PID}_1,\ \text{Trn\_id},\ \text{Dist\_id},\ \text{Seq}_{\text{OBU}}$$

(3) SM_j contacts SM_i based on the disclosed district identifier in order to validate the session parameters which the user claims to hold. The link is considered to be secured between interconnected SMs.

$$\text{SM}_\text{j} \rightarrow \text{SM}_\text{i} : \text{Enc}\{\text{SS\_id},\ \text{PID}_1,\ \text{Trn\_id},\ \text{Dist\_id},\ \text{Seq}_{\text{OBU}}\}_{K_{\text{SM}_\text{j}-\text{SM}_\text{i}}}$$

(4) SM_i responds the request to SM_j. If the validation succeeds, a successful message is released (RSP);

DOI: 10.1002/sec

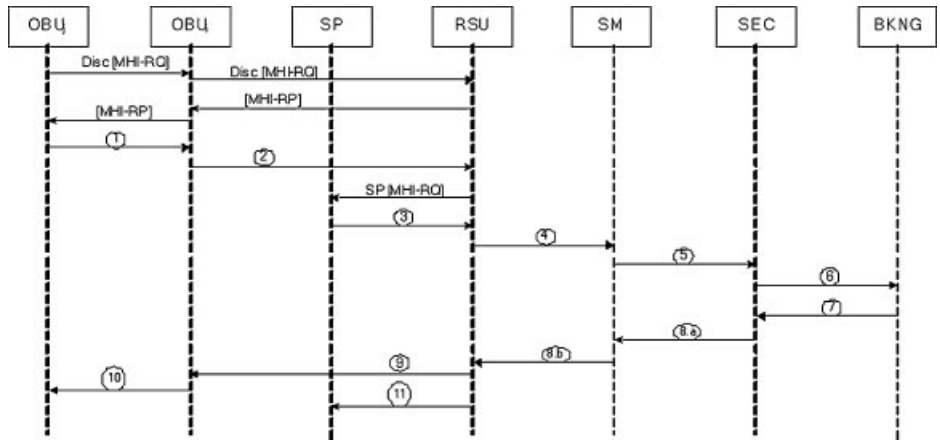

Fig. 5. MHI-RQ exchange messages.

otherwise, a denial message is issued.

$$\mathrm{SM_i} \rightarrow \mathrm{SM_j} : \mathrm{Enc}\left\{\mathrm{RSP},\ \mathrm{SS\_id_i},\ \mathrm{Dist\_id_j},\ \mathrm{PID_1},\ \mathrm{Seq_{OBU}}\right\}_{K_{\mathrm{SM_j}-\mathrm{SM_i}}}$$

(5) Once a positive response is received at the new district domain, a new temporary register is created at $\mathrm{SM_j}$ to continue offering the service in the new domain. The composed message is encrypted by using the OBU's public key which includes the successful response, new session ID at district j, temporary user, and increased sequence number.

$$\mathrm{SM_j} \rightarrow {}_a\mathrm{RSU_j} \rightarrow_b \mathrm{OBU} : \mathrm{Enc}\left\{\mathrm{RSP},\ \mathrm{SS\_id_j},\ \mathrm{Distr\_id_j},\ \mathrm{PID_1},\ \mathrm{Seq_{OBU}}\right\}_{K_{\mathrm{OBU}}}$$

Figure 4 shows the exchange of messages for the EC-RQ protocol. Notice that in the EC-RQ protocol the active participation of the service provider (SP) is not required to corroborate information between different service district domains. The relay of current service parameters is done by the corresponding SMs of each district domain.

3.3. Multi-Hop Initiation Request Protocol [MHI-RQ] for On-Demand Services

This protocol covers the initial service request protocol suitable for multi-hop environments. We consider that there must be an exchange of public keys and validation of digital signatures for intermediate nodes in the multi-hop forwarding. The MHI-RQ protocol follows the same validation steps as those performed in the SHI-RQ (see Figure 5); however, additional considerations to foster participation among forwarding nodes need to be defined. An MHI-RQ request is first transmitted after a forwarding chain has been established to reach the broadcasting RSU. This forwarding chain consists of all participating nodes that agree to deliver messages between the final recipients up to the fixed network. The establishment of the forwarding chain is assumed to be part of the discovery mechanism in a multi-hop propagation mode within a single district domain.

(1) Given the fact that message delivery has to pass through different intermediate nodes, $\mathrm{OBU_i}$ sends an encrypted MHI-RQ request by using the RSU's public key, previously retrieved during the discovery process, so that way for intermediate nodes cannot retrieve sensitive information from the source. The request message contains the service identifier, protected banking credential, and sequence number. Additionally, the source public certificate is appended to the message.

$$\mathrm{OBU_i} \rightarrow \mathrm{OBU_j} : \mathrm{Enc}\left\{\mathrm{Srv\_id},\ \mathrm{Enc}\left\{\mathrm{Bnk\_id}\right\}_{K_{\mathrm{bnk}-\mathrm{obu}}},\ \mathrm{Seq_{OBU_i}}\right\}_{K_{\mathrm{RSU}}},\ \mathrm{Cert_{OBU_i}}$$

(2) $\mathrm{OBU_j}$ is the anchor node which communicates directly to the RSU. $\mathrm{OBU_j}$ relays the information received from $\mathrm{OBU_i}$ to the local RSU. Recall that intermediate nodes attach their public certificates which will serve at the BNK for the generation of

DOI: 10.1002/sec

incentives.

$$\mathrm{OBU_j} \rightarrow \mathrm{RSU}: \mathrm{Enc}\left\{\mathrm{Srv\_id},\ \mathrm{Enc}\{\mathrm{Bnk\_id}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Seq_{OBU_i}}\right\}_{K_{\mathrm{RSU}}},\ \mathrm{Cert_{OBU_i}},\ \mathrm{Cert_{OBU_j}}$$

(3) The RSU sends a request message to the corresponding SP based on the service identifier provided by the requester. The SP replies with its public certificate and a sequence number.

$$\mathrm{SP} \rightarrow \mathrm{RSU}: \mathrm{Cert_{SP}},\ \mathrm{Seq_{SP}}$$

(4) The RSU collects the data coming from the forwarding chain, as well as, the SP and relays the decrypted message to the SM.

$$\mathrm{RSU} \rightarrow \mathrm{SM}: \mathrm{Cert_{SP}}, \mathrm{Cert_{OBU_j}},\ \mathrm{Cert_{OBU_i}},\ \mathrm{Srv\_id},\ \mathrm{Enc}\{\mathrm{Bnk\_id}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Seq_{OBU_i}},\ \mathrm{Seq_{SP}}$$

(5) The SM creates a new session identifier for the prospective session. Additionally, the SM relays the received the data which contains the public certificates of all participating nodes to the SEC for their validation. If any holder in the chain of public certificates is found to have a revoked status in the CRL, the processing of the service request is aborted.

$$\mathrm{SM} \rightarrow \mathrm{SEC}: \mathrm{Cert_{SP}},\ \mathrm{Cert_{OBU}}, \mathrm{Cert_{OBU_i}},\ \mathrm{Srv\_id},\ \mathrm{Enc}\{\mathrm{Bnk\_id}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Seq_{OBU_i}},\ \mathrm{Seq_{SP}}$$

(6) The SEC module relays the user's banking parameters for their validation at the banking entity.

$$\mathrm{SEC} \rightarrow \mathrm{BNK}: \mathrm{Cert_{OBU_j}},\ \mathrm{Cert_{OBU_i}},\ \mathrm{SS\_id},\ \mathrm{Srv\_id},\ \mathrm{Enc}\{\mathrm{Bnk\_id}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Seq_{OBU_i}}$$

(7) In the BKN, the user will be charged according to the service requested. If validation is successful, the BNK generates credit units for the requester, as well as, bonus units for each participating node which can serve for later rewards. The credit unit for the user is encrypted by using a pre-established shared secret key while bonus credentials are encrypted by using the public key for each corresponding intermediate node. Additionally, a transaction identifier and a timestamp are generated.

$$\mathrm{BNK} \rightarrow \mathrm{SEC}: \mathrm{Cert_{OBU_j}},\ \mathrm{Cert_{OBU_i}},\ \mathrm{SS\_id},\ \mathrm{Srv\_id},\ \mathrm{Enc}\{\mathrm{Bns}\}_{K_{\mathrm{OBU_j}}},\ \mathrm{Enc}\{\mathrm{Crd\_unt}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Trn\_id},\ \mathrm{T},\ \mathrm{Seq_{OBU_i}}$$

(8) The SEC relays the message to the SM. The information intended for the SP is encrypted with a shared secret key between the SP and the SEC, while the information intended for the user is encrypted with its public key. This encrypted message includes the session key, temporary user ID, encrypted credit units, transaction identifier, timestamp, and sequence number. The bonus credential for the intermediate nodes is appended to the secured composed message.

$$\mathrm{SEC} \rightarrow_a \mathrm{SM}(1) \rightarrow_b \mathrm{RSU}: \mathrm{Enc}\left\{\mathrm{PID_1},\ \mathrm{Dist\_id},\ \mathrm{SS\_id},\ \mathrm{Kss},\ \mathrm{Enc}\{\mathrm{Crd\_unt}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Trn\_id},\ \mathrm{Seq_{OBU_i}}\right\}_{K_{\mathrm{OBU}}}\ \mathrm{Cert_{OBU_j}},\ \mathrm{Cert_{OBU_i}},\ \mathrm{Enc}\{\mathrm{Bns}\}_{K_{\mathrm{OBU_j}}}$$

$$\mathrm{SEC} \rightarrow_a \mathrm{SM}(2) \rightarrow_b \mathrm{RSU}: \mathrm{Enc}\left\{\mathrm{PID_2},\ \mathrm{SS\_id},\ \mathrm{Kss},\ \mathrm{Trn\_id},\ \mathrm{T},\ \mathrm{Seq_{SP}}\right\}_{K_{\mathrm{SP}}}$$

(9) RSU relays session parameters to $\mathrm{OBU_j}$ which serves as an anchor point for the multi-hop mode to the fixed infrastructure. $\mathrm{OBU_j}$ retrieves its bonus units by decrypting it with its private key.

$$\mathrm{RSU} \rightarrow \mathrm{OBU_j}: \mathrm{Enc}\left\{\mathrm{PID_1},\ \mathrm{Dist\_id},\ \mathrm{SS\_id},\ \mathrm{Kss},\ \mathrm{Enc}\{\mathrm{Crd\_unt}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Trn\_id},\ \mathrm{T},\ \mathrm{Seq_{OBU_i}}\right\}_{K_{\mathrm{OBU}}}\ \mathrm{Cert_{OBU_i}},\ \mathrm{Cert_{OBU_j}},\ \mathrm{Enc}\{\mathrm{Bns}\}_{K_{\mathrm{OBU_j}}},\ \mathrm{Cert_{RSU}}$$

(10) The message is forwarded through the multi-hop environment to its final destination.

$$\mathrm{OBU_j} \rightarrow \mathrm{OBU_i}: \mathrm{Enc}\left\{\mathrm{SS\_id},\ \mathrm{PID_1},\ \mathrm{Kss},\ \mathrm{Enc}\{\mathrm{Crd\_unt}\}_{K_{\mathrm{bnk-obu}}},\ \mathrm{Trn\_id},\ \mathrm{T},\ \mathrm{Seq_{OBU_i}}\right\}_{K_{\mathrm{OBU}}},\ \mathrm{Cert_{OBU_i}}$$

DOI: 10.1002/sec

(11) The RSU sends the corresponding session parameters to SP which includes the shared session key.

$$\text{RSU} \rightarrow \text{SP}: \text{Enc}\left\{\text{SS\_id},\ \text{PID}_2,\ \text{Kss},\ \text{Trn\_id},\ \text{T},\ \text{Seq}_{\text{SP}}\right\}_{K_{\text{SP}}}$$

Figure 5 shows the exchange of messages for the MHI-RQ protocol.

4. Analytical Model

In this section, we analyze the signaling cost related to the service request messages when each sub-protocol takes place. First, we define the cost variables regarding data processing by each tier process involved in the district domain architecture, as well as, the link cost for the propagation medium and the cost related to performing cryptographic operations. Note that we define the term signaling cost as the cost due to an exchange of control messages to allow access to services and which are not part of the service payload. Table II enlists the symbols for the corresponding cost values and their definitions.

In the following we analytically calculate the total signaling cost for each set of request messages.

A. Signaling cost for SHI-RQ messages is expressed as

$$C_{\text{OBU}} = 4 * w_l + 3 * C_1 + S_{\text{ET}} + S_{\text{DT}} + S_X + S_{\text{ES}} + S_{\text{DS}} \quad (1)$$

Table II. Cryptographic, link, and processing costs.

Symbol	Definition
w_l	Wireless link cost to wireless infrastructure
θ	Wired link cost: SP and RSU
ρ	Wired link cost: RSU and district domain
w_a	Wireless link cost *ad hoc* medium
α	Wired link cost within a district domain
η	Wired link cost for domain interconnection
Data access processing cost	
C_1	OBU data access processing cost
C_2	SP data access processing cost
C_3	RSU data access processing cost
C_4	SM data access processing cost
C_5	SEC data access processing cost
C_6	BNKG data access processing cost
Cryptographic cost	
S_{ES}	Encryption cost by using public keys
S_{ET}	Decryption cost by using private keys
S_{DS}	Encryption cost by using secret shared keys
S_{DT}	Decryption cost by using secret shared keys
S_y	Related cost for validating signatures
S_x	Related cost for generating signatures
S_z	Related cost for generating pseudonyms

$$C_{\text{RSU}} = 4 * C_3 + 2 * \rho + S_{\text{ET}} + S_{\text{DT}} + 2 * S_Y \quad (2)$$

$$C_{\text{SP}} = 2 * C_2 + 2 * \theta + S_X \quad (3)$$

$$C_{\text{SM}} = 2 * \alpha + 2 * C_4 \quad (4)$$

$$C_{\text{SEC}} = 2 * \alpha + 2 * C_5 + 2 \times (S_{DT} + S_{ET} + S_y + S_x + S_z) \quad (5)$$

$$C_{\text{BNKG}} = C_6 + S_{\text{DS}} + S_{\text{ES}} \quad (6)$$

where the total signaling cost for a SHI-RQ request becomes

$$C_{\text{SHI-RQ}} = C_{\text{OBU}} + C_{\text{RSU}} + C_{\text{SP}} + C_{\text{SM}} + C_{\text{SEC}} + C_{\text{BNKG}} \quad (7)$$

B. Signaling cost for an EC-RQ message is expressed as

$$C_{\text{OBU}_\text{i}} = 4 * w_l + 3 * C_1 + S_{\text{ET}} + S_{\text{DT}} + S_X \quad (8)$$

$$C_{\text{RSU}_\text{j}} = 2 * C_3 + 2 * \rho + S_{\text{ET}} + S_{\text{DT}} + S_Y \quad (9)$$

$$C_{\text{SM}_\text{j}} = 2 * C_4 + 2 * \eta + S_{\text{ES}} + S_{\text{DS}} \quad (10)$$

$$C_{\text{SM}_\text{i}} = C_4 + S_{\text{ES}} + S_{\text{DS}} \quad (11)$$

where the total signaling cost for an EC-RQ request becomes

$$C_{\text{EC-RQ}} = C_{\text{OBU}'_\text{i}} + C_{\text{RSU}_\text{j}} + C_{\text{SM}_\text{j}} + C_{\text{SM}_\text{i}} \quad (12)$$

C. Signaling cost for a MHI-RQ message is expressed as

$$C_{\text{OBU}_\text{i}} = 4 * w_a + 3 * C_1 + S_{\text{ET}} + S_{\text{DT}} + S_X + S_{\text{ES}} + S_{\text{DS}} \quad (13)$$

$$C_{\text{OBU}_\text{j}} = 2 * w_l + 3 * C_1 + S_X + S_Y + S_{\text{DT}} \quad (14)$$

$$C_{\text{RSU}} = 4 * C_3 + 2 * \rho + S_{\text{ET}} + S_{\text{DT}} + 3 * S_Y \quad (15)$$

DOI: 10.1002/sec

$$C_{\mathrm{SP}} = 2 * C_2 + 2 * \theta + S_X \tag{16}$$

$$C_{\mathrm{SM}} = 2 * \alpha + 2 * C_4 \tag{17}$$

$$C_{\mathrm{SEC}} = 2 * \alpha + 2 * C_5 + 2 \times (S_{\mathrm{DT}} + S_{\mathrm{ET}} + S_y + S_x + S_z) \tag{18}$$

$$C_{\mathrm{BNKG}} = C_6 + S_{\mathrm{DS}} + S_{\mathrm{ES}} + S_{\mathrm{ET}} \tag{19}$$

where the total signaling cost for a MHI-RQ request becomes as:

$$C_{\mathrm{MHI-RQ}} = C_{\mathrm{OBU_i}} + C_{\mathrm{OBU_j}} + C_{\mathrm{RSU}} + C_{\mathrm{SP}} + C_{\mathrm{SM}} + C_{\mathrm{SEC}} + C_{\mathrm{BNKG}} \tag{20}$$

Notice that the total cost for each signaling protocol becomes the cumulative cost of each participating tier element. A single initial request will have a total cost of $C_{\mathrm{SHI-RQ}}$ to deliver session parameters to the user. In the case of requesting an extension of service delivery within a new district domain, the total cost becomes $C_{\mathrm{EC-RQ}}$. In the multi-hop mode, $C_{\mathrm{MHI-RQ}}$ represents the total signaling cots for a single service request when a multi-hop mode is used.

4.1. Mobility Model

Given the fact that vehicles can have high mobility and a dynamic behavior, there can be different vehicle mobility scenarios that the service district domain has to be able to successfully deliver services at. For instance, if a user gets attached to a RSU, that user must be able to request and maintain an on-demand service session within the coverage area of that district domain. As the service district domain can manage several RSUs under its jurisdiction, the user should be able to maintain its service session when there is a transition between adjacent RSUs under the same district domain. Additionally, the interaction between adjacent service districts domains are intended to maintain mid to long-term sessions, by sharing information of active session parameters through multiple district domains. Finally, a scenario in the multi-hop environment can be considered where a vehicle requests a service session when it is out of the radio transmission coverage of the closest RSU.

For the numerical analysis presented hereafter, we consider the fluid model [12] to characterize the mobility behavior of vehicles when traversing different service coverage areas. The coverage areas are assumed to be circular and contiguous and with a node direction uniformly distributed [0,2 π) [13]. First, we define the border crossing rate out of the coverage area within a single RSU in the incumbent service district domain as expressed in Reference [14]:

$$\mu_s = \frac{\pi v}{4R_s} \tag{21}$$

where R_s is the radius of the circular area of the transmitting RSU and v is the average vehicle speed. The border crossing rate out of the serving district domain to an adjacent one is given by

$$\mu_m = \frac{\pi v}{4R_m} \tag{22}$$

where R_m is the radius of the serving district domain. The border crossing rate for the vehicle that stays without changing district domains is given by

$$\mu_s - \mu_m = \frac{\pi v}{4}\left(\frac{1}{R_s} - \frac{1}{R_m}\right) \tag{23}$$

To evaluate the total signaling cost, we need to consider the effect of interdomain mobility which includes the values of the respective border crossing rates (μ_s and μ_m). The total cost expression includes the cost values for executing the SHI-RQ and the EC-RQ protocols, as well as, the impact of the border crossing rates, vehicle density and the service area.

$$\begin{aligned} C_T &= \rho * A(C_{\mathrm{SHI-RQ}} * N * (\mu_s - \mu_m) + C_{\mathrm{EC-RQ}} * \mu_m) \\ &= \rho * A * \frac{\pi v}{4}\left(C_{\mathrm{SHI-RQ}} * N * \left(\frac{1}{R_s} - \frac{1}{R_m}\right) + C_{\mathrm{EC-RQ}} * \frac{1}{R_m}\right) \end{aligned} \tag{24}$$

where ρ is the vehicle density as defined in Reference [15], A is the total service area and N is the number of RSUs.

Additionally, it is sometimes useful to introduce the parameter of Session to Mobility Ratio (SMR) [16] which can be defined as the relation between the session arrival rate and the RSU border crossing rate. This means that the user will be able to request a certain number of independent sessions within a district service

DOI: 10.1002/sec

domain. The SMR is expressed as follows:

$$\text{SMR} = \frac{\lambda_s}{\mu_s} \tag{25}$$

where λ_s is the session arrival rate and μ_s is the RSU border crossing rate.

4.2. Numerical Results

For the evaluation of the aforementioned signaling protocols, we calculate the related costs in terms of latency (seconds) to estimate the overall signaling cost. To the best of our knowledge, there are no other reference works which deal with accessing services in a complete tier process and estimate the related time response as we present in this study.

Given the high mobility of vehicles, latency is a determining factor in the ability of the architecture to deliver services to vehicles and maintain service sessions within and across service district domains. The list of costs is shown in Table III. For the costs of security operations, we consider the benchmark values provided by crypto++ [17] regarding the implementation of cryptographic operations. In the case of digital signatures, these are based on the RSA cryptographic scheme with a fixed length of 128 bytes. For the asymmetric encryption/decryption operations we also considered the RSA (128 bytes) scheme. Moreover, SHA-1 operations are necessary when generating temporary user identifiers/pseudonyms (32 bits) at the security module tier. We also consider the AES (128-bit key) mechanism for encryption/decryption when using shared secret keys. Furthermore, we assumed 20 ms latency for data processing at each tier element and we also set the link cost for the wireless medium at 5 ms and for the fixed network at 2 ms. Additionally, we assume an extra cost of 20 ms for data processing due to some policy and accounting operations. The latter values are considered to be reasonable for processing data operations while the values for propagation in the wireless medium (WLAN) were obtained from previous statistics in OPNET wireless modeler. Moreover, we considered a total number of RSU of 4 per district domain.

Table III. Cryptographic, link, and processing costs.

Symbol	Value in seconds (s)
w_l	0.005
θ	0.002
ρ	0.002
w_a	0.005
α	0.002
η	0.01
C_1	0.02
C_2	0.02
C_3	0.02
C_4	0.02
C_5	0.02
C_6	0.02
S_{ES}	0.031
S_{ET}	0.0013
S_{DS}	0.031
S_{DT}	0.003
S_y	0.0013
S_x	0.003
S_z	0.0878

To evaluate the signaling performance of each protocol we used Matlab. We did some initial experimentations to evaluate in Matlab the latencies introduced by the three access protocols. We observed that in the case of SHI-RQ, it would take 0.765 s for a single vehicle to receive a response from a district domain for an initial request made. For the EC-RQ, the underlying multi-hop routing protocol was considered as AODV for analysis purposes. We considered an average propagation delay between two nodes of 20 ms as experimented in Reference [18] when using AODV protocol for vehicular *ad hoc* routing.

For the EC-RQ, it would take 0.365 s when the vehicle makes a request for extended connectivity in a next neighboring district domain, and the current session parameters are shared between the SMs of the participating district domains. Additionally, as a reference point we performed further analysis by using the ACE (Application Characterization Environment) from the Opnet Wireless Modeler by feeding the same tier elements with the corresponding processing times, and the results that we observed were 0.88 and 0.41 s for SHI-RQ and EC-RQ, respectively. These results show a slight difference but we can conclude that cost expressions for the SHI-RQ and EC-RQ are consistent with the result obtained by the ACE. Now, if we consider a single RSU with a coverage radius of 250 m and a moving vehicle with maximum speed of 40 m/s (144 km/h), then the vehicle would cross the RSU's transmission range (500 m) in approximately 12.5 s. This means that the vehicle would have sufficient time to execute the SHI-RQ protocol and retrieve the corresponding session parameters from the district domain. Regarding the MHI-RQ protocol we found, that it would take 0.945 s for a vehicle in a multi-hop transmission mode comprising one intermediate hop, to request and receive secure session parameters from the serving district service domain. It is worth

DOI: 10.1002/sec

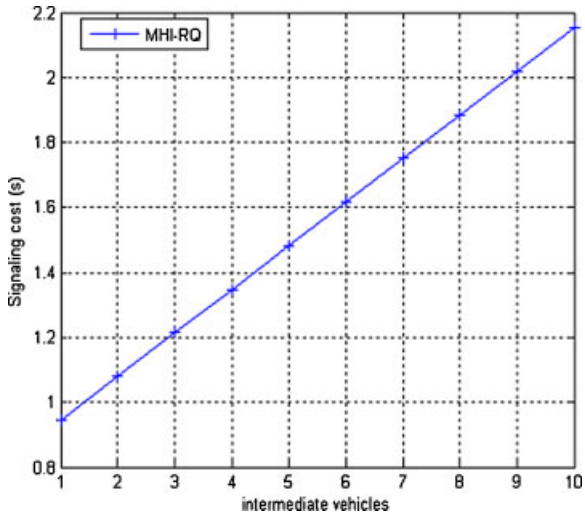

Fig. 6. Cost (s) for MHI-RQ vs. intermediate vehicles.

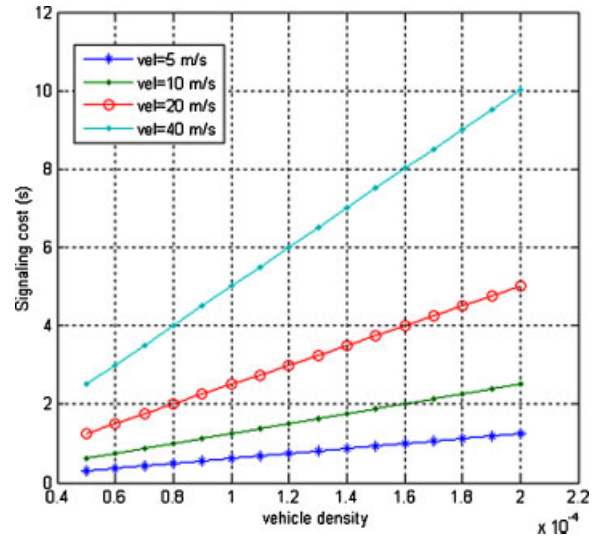

Fig. 7. Total signaling cost vs. vehicle density.

mentioning that safety applications have the highest priority and can affect the latency and scalability of the solution in high density scenarios. The referred latency can be from 50 to 100 ms for life threatening applications [19] such as safety messages triggered by events based on dangerous vehicular conditions. Safety messages are exchanged through dedicated control channels while non-safety usage in the control channel is limited to occasional advertisements of private applications in the service channels and represents no considerable impact to the overall channel load.

Figure 6 shows the performance of the overall latency for the MHI-RQ when the number of intermediate vehicles increases. With a maximum number of 10 intermediate nodes, the latency cost reaches nearly 2.2 s for a single MIH-RQ request while when there is a single intermediate node the latency cost is around .94 s. There is only one request at a time being processed by the district domain, but some additional latency is introduced at the BNK because there are more processing operations such as bonus units to be generated for each participating node. The cryptographic operations at each intermediate node are also added. The addition of intermediate nodes does impose some impact on the signaling cost, but even when the number of intermediate nodes is unlikely high, i.e., 10, this impact is still relatively acceptable with 2.2 s for 10 intermediate nodes.

The next analysis we performed deals with an increase the vehicle density at different speeds while having a direct (non-multi-hop) access to an RSU in Figure 7. Additionally, we considered the impact of the related vehicle domain border crossing rates with a district domain radius of 1 km and a RSU radius of 250 m. When the average speed increases, the border crossing rate increases for a RSU, as well as, for the district domain. As a result, a vehicle moving at high speeds will need to perform more EC-RQ requests since it travels rapidly between contiguous district domains. A relatively very high vehicle density of 0.001 which corresponds to 1000 vehicles/km^2 requesting services implies a cost of 4.5 s when vehicles are traveling at 144 km/h (40 m/s). The cost is 2.2 s when vehicles are traveling at 72 km/h

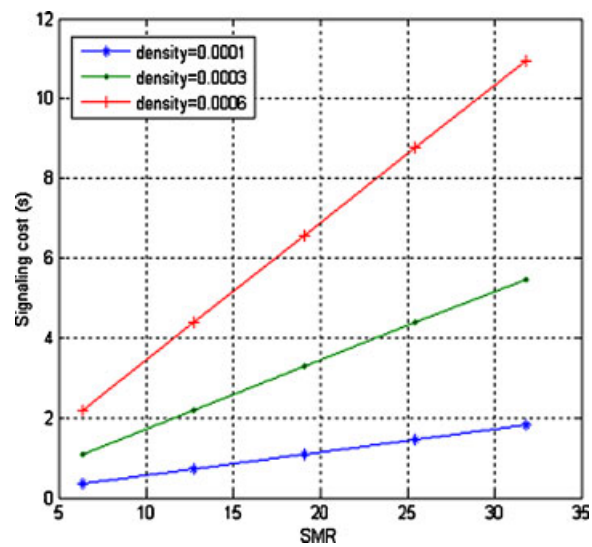

Fig. 8. Total signaling cost vs. SMR.

DOI: 10.1002/sec

(20 m/s). For a bit more realistic densities such as 500 vehicles/km^2 (0.0005 density in the Figure), latency cost remains below 1 s at most travel speeds.

Finally, in Figure 8 we observe the trend for the signaling cost against the SMR which represents the session arrival rate per border crossing rate. At a speed of 144 km/h, it is observed that a session request arrival rate higher than the rate of border crossing by a vehicle has much more impact on latency generation. At SMR values below 10, the signaling cost remains reasonable even for a very high density of vehicles of 600 vehicles/km^2. When SMR is higher than 10, the cost of signaling inherent from the independent session requests within a vehicle becomes relatively high. When shared sessions within a same vehicle are possible, they should be promoted.

5. Conclusions

In this paper, the analytical model of a secure architecture for secure service provisioning for VANETs has been presented. Three protocols for vehicle service requests have been described; SHI-RQ, EC-RQ, and MIH-RQ. When a vehicle initiates a request message in the form of a SHI-RQ request to a specific service district domain, if the validation is successful, the vehicle will be granted the corresponding session parameters which include a temporary session key as well as a credential units issued by the BNK.

When a vehicle moves from one district domain to an adjacent one, and upon the detection of the new district domain, an EC-RQ message request is sent with the objective to trigger the exchange of information between the previous and the new SM. On-going session parameters can then be extended to other service district domains. An MHI-RQ message request is sent when a vehicle initiates a service request with a multi-hop transmission mode. At the district domain, the BNK will be responsible for generating credit units for the requester as well as bonus units for each participating node. These banking credentials are encrypted by using the public certificate for each intermediate node. We analyzed the signaling cost in terms of latency for SHI-RQ, EC-RQ, and MHI-RQ protocols. We also derived the mobility model in order to assess the total signaling cost which involves the signaling within an initial district domain and when a vehicle moves to another domain. This mobility model will depend on the values of the border crossing rate for staying within a district domain and for moving out of the domain. The obtained signaling cost values remain acceptable for realistic vehicle densities within a service area, even when vehicles travel at a high speed.

Future research work might be oriented toward evaluating the impact of the choice of different categories of multi-hop routing and forwarding schemes on the signaling cost for the secure service provisioning in the architecture. One category that will particularly be considered is secure geographic multicast schemes that guarantee integrity of the data and privacy of the participating nodes.

Acknowledgements

This work has been performed with funding from the Canadian AUTO21 Network of Centers of Excellence - AUTO21, and from the Natural Sciences and Engineering Research Council of Canada.

References

1. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Networking Services. IEEE Std 1609.3^{TM}-2007.
2. Cooperative Vehicle-Infrastructure Systems, CVIS. www.cvisproject.org
3. Coronado E, Cherkaoui S. Service Discovery and Service Access in Wireless Vehicular Networks. In *Proceedings of IEEE Globecom'08*, New Orleans, USA, 2008.
4. El Zarki M, Sharad M, Tsudik G. Security Issues in a Future Vehicular Networks. In *European Wireless*. 2002.
5. Raya M, Hubaux J. The Security of Vanet. *ACM SASN'05*, USA. 2005.
6. Raya M, Papadimitratos P, Hubaux J. Securing vehicular communications. *EPFL* 2006.
7. Dotzer F. Privacy Issues in Vanet. *Workshop on Privacy Enhancing Technologies*, Croatia, 2005.
8. Moustafa H, Bourddon G, Gourhant Y. AAA in vehicular Communication on Highways with Ad Hoc Networking Support: A proposed Architecture. *VANET'05*, Germany, 2005.
9. Mohan M, Joiner L. Solving Billing Issues in Ad Hoc Networks. *ACMSE '04*, Alabama USA, 2004.
10. Buttyan L, Hubaux J. Stimulating cooperation in self-organizing mobile ad hoc networks. Kluwer. *Mobile Networks and Applications* 2003; **8**: 579–595.
11. Housley R, Polk W, Ford W, Solo D. RFC, 3280. 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile'. *Network Working Group. Internet Society*, 2002.
12. Zhang L, Pierre SR. Performance Analysis of Fast Handover for Hierarchical MIPv6 in Cellular Networks. In *Proceedings of IEEE Vehicular Technology Conference*, Canada, May, 2008.
13. Nguyen H, Harmen R. Performance Analysis of Distributed Location Management for Wireless Networks. In *Proceedings of the 15th ICOIN*, Washington, USA, 2001.
14. Wu Z. An approach for Optimizing Binding Lifetime with Mobile IPv6. *Information Technology Papers*, Bond University, Australia, 2003.

DOI: 10.1002/sec

15. Zhang X, Gomez J, Campbell A. P-MIP:Paging Extension for Mobile IP. *Mobile Networks and Applications*, Kluwer Academic Publishers, 2002.
16. Zhang L, Pierre SR. Performance Analysis of Fast Handover for Hierarchical MIPv6 in Cellular Networks. In *Proceedings of IEEE Vehicular Technology Conference*, Canada, May, 2008.
17. Crypto++, Crypto++ 5.5 Benchmarks, www.cryptopp.com/benchmarks.html 2007.
18. Eichler S, Dotzer F, Schwingenschlogl C, Fabra F, Eberspacher J. Secure Routing in a Vehicular Ad Hoc Network. *IEEE VTC*, USA, 2004.
19. Torrent-Moreno M, Hartenstein H. *Decentralized Systems and Network Services*. Institute for Telematics, University of Karlsruhe, 2005.

DOI: 10.1002/sec