Provisioning of On-demand Services in Vehicular Networks

Etienne Coronado and Soumaya Cherkaoui
Department of Electrical and Computer Engineering
Université de Sherbrooke, Quebec, Canada
Etienne.Coronado@usherbrooke.ca, Soumaya.Cherkaoui@usherbrooke.ca

Abstract—Wireless vehicular communications possess significant challenges for their massive deployment in next generation vehicular networks. Some important issues that must be tackled deal with security, billing and scalability in order to provide reliable services in the case of non-safety applications. In this paper we study a service provisioning protocol intended for Vehicular-to-Infrastructure (V2I) environments where service access is granted by administrative areas in the form of service district domains. To provide scalability of the service, it is necessary to share the current user service parameters between active district domains. Our analysis covers the average response time for requesting on-demand services as well as for sharing service parameters between district domains.

Index Terms—service provisioning, scalability, security, on-demand services

I. INTRODUCTION

Nowadays, significant research efforts, mainly oriented to the deployment of safety application in vehicular networks (VN), have been developed in conjunction by the automotive industry and academy research groups. In the case of non-safety applications, more research work needs to be done since their deployment in roadside communications could represent a huge potential in economic terms. Initial studies in VN began with standardization work of Direct Short Range Communication (DSRC) [1] which is still under development. The DSRC technology will provide bidirectional transmission of safety and non-safety messages from vehicles in transit to the roadside infrastructure in the proximity, i.e. Vehicular-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V). The success in the deployment of service provisioning models for highly mobile environments will mainly depend on the implementation of robust architectures which will be able to maintain their overall performance when facing hostile environments. These new architectures will base their resiliency on their capability to manage secure mechanisms for users who possess dynamic and sometimes anonymous behaviors. Another important issue deals with the need to provide service coverage to extensive geographic areas; therefore, considerable deployment of infrastructure would be required along the road transport network. To tackle this problem, future vehicular communications need to be scalable either when increasing the number of interactive vehicles or

In the case of V2I communications, the IEEE 1609.3 [2] trial standard for Wireless Access in Vehicular Environments (WAVE) describes the way services are announced and discovered through vehicular environment. In IEEE 1609.3 information related to specific providers and their corresponding channels are 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). Then, the WSIE frame is received and processed by transitory and potential users; and which retrieved parameters will be employed to request specific services. Applications from a provider must be registered at the WAVE management entity (WME) which includes information such as channel of operation, address information, description of the services being offered and application priority.

From the aforementioned service discovery process, some challenges might arise concerning the request of services by potential clients without being attached to any sort of home network service infrastructure. For instance, this can be case where unknown users are willing to retrieved services from the neighboring roadside infrastructure. Under these circumstances, service models offered on the roadside infrastructure are likely to be considered as spontaneous on-demand services. Based on this premise, it is possible to assume that service providers have poor or even no knowledge of transitory users whenever a service request is executed. However, exchanges of information between transitory users and service providers must be kept reliable and secure, especially, when sensitive information is transferred such as financial transactions or even disclosure of user identities.

In our study we perform further analysis from the work presented in [3] which is intended to provide support spontaneous on-demand service provisioning for vehicular networks. Section II describes the service provisioning protocol for vehicle-to-infrastructure (V2I) and which covers the corresponding signaling costs. Section III presents simulation results based on different scenarios as it finishes with the conclusions.
II. SCALABLE SERVICE PROVISIONING IN VEHICULAR ENVIRONMENTS

As mentioned before, the deployment of reliable information services along the roadside infrastructure must be robust and scalable. The proposed service provisioning protocol must rely in a service district domain architecture which main function is to validate and grant network and service access to spontaneous “on-demand” requesters within its geographic jurisdiction. In the following, it is described a district domain service architecture as illustrated in Figure 1.

Security module. 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 the real identities of vehicles; while the PA is in charge of generating secure cryptographic material for specific service sessions [4]. As proposed in [5;6;7] prospective vehicles are likely to have installed a tamper resistant device which contains a set of preloaded cryptographic material either issued by official transport authorities or car manufacturers. Now, within a district domain any disclosed public key certificate is subjected to verification. Verification of the user’s public certificate is based on public Certificate Revocation List (CRL) [8] which contains a list of serial numbers of revoked official public key certificates, as well as, the corresponding validation of their digital signatures. Notice that authentication is based on the certainty of the current requester’s certificates and not by user-id/password based authentication. This type of validation will promote the request of spontaneous on-demand services. Additionally, the security module generates the corresponding session keys (Kss) for both the user and service provider. Moreover, a set of pseudonyms (PID) are generated and which can serve as temporary identifiers for both the user and the service provider; where these pseudonyms are valid only during the active service session.

Banking module. Depending on the services requested, it is required the presence of banking entities which need to be in place 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 banking module. This billing entity shall be responsible for the issuance of on-demand credit units which are the credentials that allow the right to use for specific information services. We assume that there must be a pre-established relationship between the banking entity and the user for validation purposes which can be based on a special type of banking credential pre-assigned off-line. This kind of banking validation can resemble a credit-card payment model where the affordability of the user to acquire a specific service can be verified. Once a successful response is retrieved, the banking entity is able to dispatch the corresponding credit units and transaction identifiers which can specify the amount of content data to be retrieved or the maximum time duration for the service session.

Session manager. Regarding the presence of the session manager, its main function is to establish associations with other external session managers 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 session managers. This module is also responsible for creating a session ID and for collecting all the session parameters before being forwarded 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. Some parameters are temporary user identifier (pseudonym), a session identifier, 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.

Policy module. The execution of service policies defines the way how information is treated based on their 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.

A. Vehicle to infrastructure service access

The exchange of messages necessary to request access to announced services between the potential user and the fixed network is depicted in Figure 2.
From the above figure, a transitory OBU (user) sends an initial message to the RSU notifying its presence as denoted in arrow 1. Then, the RSU replies the message by requesting the OBU’s attributes and expecting to receive the OBU’s public key certificate, timestamp, the service identifier retrieved from the PST list and protected banking credentials as depicted in arrows 2 and 3. The RSU contacts the specific SP based on the service identifier in order to retrieve the SP’s attributes which include the SP’s public key certificate through arrows 4 and 5. The collected information from both the OBU and SP is sent to the session manager where a session ID is generated (arrow 6). Once this is done, the SEC module receives the request in arrow 7 where key certificates need to be verified if they do not possess a revoked status. As soon as this validation is retrieved, this module is able to generate the session key for the OBU and the provider, as well as, the corresponding pseudonyms. A check of the current service policies is performed at the policy module based on the service identifier through arrow 8. After this, a verification of the disclosed banking credentials is performed at the banking module where the status of its affordability is checked and if successful it creates a transaction identifier and the credential units for that service (arrow 9). For accounting purposes, temporary registers and associations for both the user and service provider are created while it is authorized for that specific session request (arrow 10). At this point, all the parameters generated for that session are collected, protected and sent back to the corresponding recipients which are both the OBU and the SP, respectively (arrows 12 to 16). Upon receiving the resulting composed message, a secure service delivery process can take place by employing the active secret session key between the OBU and the service provider. Table I enlists the corresponding service session parameters considered within the access service protocol.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID1</td>
<td>User pseudonym</td>
</tr>
<tr>
<td>PID2</td>
<td>Provider pseudonym</td>
</tr>
<tr>
<td>Kss</td>
<td>Session key</td>
</tr>
<tr>
<td>CertOBU</td>
<td>User public certificate</td>
</tr>
<tr>
<td>Cr_unct</td>
<td>Credit bonus unit</td>
</tr>
<tr>
<td>K_total_obu</td>
<td>Shared key: bank-OBU</td>
</tr>
<tr>
<td>K_sp</td>
<td>SP’s public key</td>
</tr>
<tr>
<td>K_obe</td>
<td>User public key</td>
</tr>
<tr>
<td>Ss_id</td>
<td>Session ID</td>
</tr>
<tr>
<td>Srv_id</td>
<td>Service ID</td>
</tr>
<tr>
<td>Trn_id</td>
<td>Transaction identifier</td>
</tr>
<tr>
<td>T</td>
<td>Expiration time</td>
</tr>
<tr>
<td>CertRSU</td>
<td>RSU certificate</td>
</tr>
<tr>
<td>CertSp</td>
<td>Service provider certificate</td>
</tr>
<tr>
<td>Dist_id</td>
<td>District ID</td>
</tr>
<tr>
<td>Seq</td>
<td>Sequence number</td>
</tr>
</tbody>
</table>

The resulting composed message for the OBU containing its related session parameters (table I) is protected by using the OBU’s public key.

\[
RSU \rightarrow OBU : Enc\{PID_1, SS\_id, Dist\_id, Kss, T, \\
Enc\{Crd\_unct\}_{K_{sp-obs}}\_Trn\_id, Seq_{OBU}\_K_{OBU}\_Cert_{RSU}\}
\]

While the resulting composed message received at the SP is protected by using the SP’s public key.

\[
RSU \rightarrow SP : Enc\{PID_2, SS\_id, Kss, Trn\_id, T, \\
Seq_{SP}\_K_{sp}\_Cert_{RSU}\}
\]

B. Supporting scalability

In order to provide scalable solutions, it is required the exchange of control messages between adjacent service domains where information of active service parameters is shared among operating session managers. For this reason, interconnection mechanisms need to be established at a logical level between neighboring district domains. In particular, it is necessary to include mechanisms to facilitate the exchange of information as shown in figure 2 (arrows 5 and 6). This will allow service parameters from an active session to be shared between two concurrent district domains in order to maintain an active session alive without the need for the user to be registered in a new session at the new district domain. When multiple districts are involved, a chain of relayed districts is formed in order to distribute updated information among the chain path. Moreover, a mesh connectivity topology between districts might be required to support more reliable access availability and continuity in the service.
The resulting composed message is protected by using the OBU’s public key and can be defined as:

\[ RSU_j \rightarrow OBU : Enc(SS\_id, Distr\_id_j, PID_1, Seq_{OBU_j} \}_{K_{OBU}} \]

where \( j \) represents the relayed parameters at the new district domain.

**C. Cumulative signaling cost**

In order to analyze the proposed communication model, it is possible to generalize the cumulative signaling cost based on the sum of individual cost at each tier process. Table 2 enlists the related processing costs for performing data processing, cryptographic operations and the related link costs. For simplicity purposes it is assumed the same link cost for all the network elements in the fixed network.

![Diagram of the communication model](image)

**III. SIMULATIONS OF THE COMMUNICATION MODEL**

For this analysis we employed the Application Characterization Environment ACE® whiteboard tool from the OPNET® modeler P14.5 wireless suite [9]. The ACE whiteboard is a robust tool suitable to evaluate the behavior of different tier processes within a simulation networking environment. For study purposes, we consider the cumulative processing time at each stage of the communication model involves the execution of data processing and cryptographic operations. The cryptographic processing time values are based on the benchmark speeds given in [10] for different cryptographic schemes as shown in table III. We use these time values as references in order to estimate the total response time during a simulated on-demand requesting process. The deployment of the ACE tier process in the topology network will result in the estimation of the total average response time while considering the processing time at each tier process.

**TABLE II**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( w_l )</td>
<td>wireless link cost</td>
</tr>
<tr>
<td>( w_d )</td>
<td>wired link cost</td>
</tr>
</tbody>
</table>

**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
- \( C_5 \) Policy data processing cost
- \( C_6 \) BNKG data access processing cost
- \( C_7 \) Accounting data processing cost
- \( C_8 \) Authorization data processing cost

**Cryptographic cost**

- \( \beta_0 \) OBU’s cryptographic cost
- \( \beta_{\omega} \) RSU’s cryptographic cost
- \( \beta_{\lambda} \) SM’s cryptographic cost
- \( \beta_{\lambda} \) BNKG’s cryptographic cost
- \( \beta_{\alpha} \) SP’s cryptographic cost
- \( \beta_{\psi} \) SEC’s cryptographic cost

Based on the flow diagram in Figure 2, the signaling cost at each tier process considers the number of times received messages are processed; additionally, it also considers if cryptographic operations are involved at that tier and the related cost due to wireless or wireline links. The individual signaling cost at each tier process can be expressed from equation 1 to 9.

\[
\begin{align*}
C_{OBU} &= C_1 + 2 * w_l + \beta_0 \\
C_{RSU} &= C_3 + 3 * w_d + 2 * w_l + \beta_{\omega} \\
C_{SP} &= C_2 + w_d + \beta_{\omega} \\
C_{SM} &= C_4 + 2 * w_d \\
C_{SEC} &= C_5 + 2 * w_d + \beta_{\psi} \\
C_{POL} &= C_6 + 2 * w_d \\
C_{BNKG} &= C_7 + 2 * w_d + \beta_{\lambda} \\
C_{ACC/AUTH} &= C_8 + w_d + C_9 
\end{align*}
\]

Therefore, the general expression to define the total signaling cost for requesting access within a single service district domain can be expressed.

\[
C_{Total} = C_{OBU} + C_{SP} + C_{RSU} + C_{SM} + C_{SEC} + C_{BNKG} + C_{POL} + C_{AUTH/ACC} \tag{9}
\]

To share active session information between adjacent district domains, the total signaling cost for performing the exchange of session parameters can be expressed from equation 10 to 14.

\[
\begin{align*}
C_{OBU_i} &= C_1 + 2 * w_l + \beta_0 \\
C_{RSU_j} &= C_3 + 2 * w_d + w_l + \beta_{\omega} \\
C_{SM_i} &= C_4 + 2 * w_d + \beta_{\lambda} \\
C_{SM_j} &= C_4 + w_d + \beta_{\lambda} 
\end{align*}
\]

Hence, the total signaling cost for requesting for two district domains is as follows.

\[
C_{EXCH} = C_{OBU_i} + C_{RSU_j} + C_{SM_i} + C_{SM_j} \tag{14}
\]
vehicles are 0.855 s, 0.856 s, 0.857 s and 0.862 s, within a single district for a single, 10, 20 and 50 concurrent average response time for an on-demand service request along with a uniform starting time from 110 to 120 s with a total simulation time of 130 s. As shown in Figure 6, the average response time for two active district domains is about .31 s while the average response time experienced for three active district domains reaches .48 s. As can be expected the response time to execute a service request within a single district domain is larger than the response time resulting from the exchange of information between different active district domains for an ongoing service session.

From the previous table, digital signatures are based on the RSA cryptographic algorithm with a fixed length of 128 bytes, as well as, the corresponding signature verification processes performed at the tier processes. For the OBU, SP, BNKG and SM tiers, it is needed to perform RSA (128 bytes) encryption and decryption operations. Moreover, HMAC operations are necessary when generating pseudonyms (32 bits) and for key generation, the Diffie-Hellman (DH) algorithm can be employed at the SEC tier. It is assumed a maximum packet length of 1024 bytes and TCP as a transport layer.

Furthermore, we assume 20 ms of data processing at each tier stage. That is, every time a message arrives to an specific tier it takes 20 ms to process it. The related propagation time imposed by the wireless and wireline mediums is implicitly estimated by simulator statistics results. The type of links deployed in the fixed network is set to T-base 10 for the Ethernet based subnets and DS3 links for the WAN sections (see Figure 4). The system performance will have a direct impact on the number of network connectivity devices such as access and distributions routers, as well as, as layer 2 switches.

In our setup, we set three WLAN access points which are equally distributed to cover a range of 1000 m each. Furthermore, we consider that each antenna belongs to a different service district domain. We also assume a constant speed of 50 km/h for the vehicles which can be found in a typically dense urban area. In order to represent a vehicle, we deploy a mobile node element which contains an active wireless interface and will be able to communicate with the access point.

The scope of our simulation is to determine the response time when executing the tier process for requesting on-demand services within a network. Notice that our aim is not intended to deem the time required for link discovery at lower layers but to estimate the response time when accessing services in a single and multiple district domains.

In the first setup scenario, we simulated the response time within a single district domain. The simulated ACE tier process is executed whenever a vehicle requests an on-demand session service. In order to get a reliable average response time, the ACE application was set to have a uniform repetition time between 1 and 3 s. The simulation execution was set with a uniform starting time from 10 to 20 s with a total simulation time of 80 s. As can be seen in Figure 5 the average response time for an on-demand service request along within a single district for a single, 10, 20 and 50 concurrent vehicles are, 0.855 s, 0.856 s, 0.857 s and 0.862 s, respectively. We observed that there is no significant impact on the average response time when the number of vehicles increases. Figure 6 shows the throughput in the wireless medium has its maximum level for 50 users with a highest peak level up to 13 Mb/s at 40 s. Conversely, the lowest throughput belongs for a single vehicle with more than 500 kb/s within the overall simulation time.

The second set of simulations involves the analysis of the average response time when a vehicle request extension connectivity to the adjacent access point which belongs to the second district domain. For this setup, a tier process which represents the share of information between the new and previous session managers is established. Furthermore, the interaction of a third district domain is set through a tier process that represents the interaction between the three district domains. The simulation was set with a uniform starting time from 110 to 120 with a total simulation time of 130 s. As shown in Figure 6, the average response time for two active district domains is about .31 s while the average response time experienced for three active district domains reaches .48 s. As can be expected the response time to execute a service request within a single district domain is larger than the response time resulting from the exchange of information between different active district domains for an ongoing service session.

From the results obtained in the previous simulations, we observed that the response time values for process request-response between a vehicle and the service district domains are acceptable even when increasing the number of vehicles. That is, with a speed of 50 km/h the time to transverse from side to side the coverage area it would be 72 s; where in most of this time, the user might be able to execute at least one request of access for on-demand services. That means that a user can initiate a service request at any district infrastructure as long as the vehicle remains in the current service coverage area. For district intercommunication, the average response time for exchanging information between session managers remains also acceptable.

<table>
<thead>
<tr>
<th>TABLE III</th>
<th>BENCHMARK REFERENCES FOR SECURITY OPERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation schemes</td>
<td>Processing Time (ms) per operation</td>
</tr>
<tr>
<td>RSA 1024 signature</td>
<td>1.42</td>
</tr>
<tr>
<td>RSA 1024 verification</td>
<td>0.07</td>
</tr>
<tr>
<td>RSA 1024 encryption</td>
<td>0.07</td>
</tr>
<tr>
<td>RSA 1024 decryption</td>
<td>1.52</td>
</tr>
<tr>
<td>DH 1024 key generation</td>
<td>0.44</td>
</tr>
<tr>
<td>HMAC(SHA-1)</td>
<td>6.279/byte</td>
</tr>
</tbody>
</table>

Figure 4. Network topology using Opnet Wireless Modeler.
IV. CONCLUSION

The major concern in vehicular networks is the need to provide robust and secure access to services where reliable delivery of information between vehicles and providers must be guaranteed. Our study is oriented to provide a service architecture based on the concept of district domains which are entities responsible for dispatching service parameters to on-demand users within an administrative domain. The service protocol comprises the presence of security entities, session manager, accounting, authorization and banking modules. The main goal of the security module is to verify the certainty of the holder's key certificates by using public and private certificate revocation lists. Additionally, the security module must generate the corresponding security attributes for both the requesting user and the solicited provider. One of the main parts for service provisioning model deals with the implementation of session managers which are responsible for facilitating the transference of existing and valid session parameters to other session managers located at different district domains. The communication between active session managers will help to extend service connectivity for an active user when moving through different district domains.

From our simulations, we evaluated the average response time for a user to request a secure session, as well as, the average response time for a user to request an extension of the service to a new district domain. The results showed that the average response time for on-demand requests in a single district domain are acceptable even when increasing the number of vehicles. Finally, it is worth to emphasize that more research work from the research community must be focused in the development of commercial roadside services which can be accessible, reliable and secure.

ACKNOWLEDGMENT

This work has been performed within the project “Vehicle Communications and Applications”, which is funded by the Canadian AUTO21 Network of Centers of Excellence.

REFERENCES