International Journal of Emerging Engineering Research and Technology
Volume. 2, Issue 2, May 2014, PP 213-219

Sighting and Admission of Service in Wireless Vehicular Networks

Ms.V.Vidhya
Assistant Professor, Department of CSE
AnnaiVailankanni College of Engineering
vidhyya.v@gmail.com

Mr.G.Jeyaram
Assistant Professor, Department of CSE
AnnaiVailankanni College of Engineering
jeyaramgj@gmail.com

Abstract: *Robust and reliable service architectures must be designed to guarantee the success of future vehicular networks. This paper addresses service provisioning elements such as communication service models, service sighting and service admission intended for vehicular environments. We propose a secure service admission architecture based on the concept of district domains which are entities responsible for dispatching session parameters to on-demand users. The service architecture comprises the presence of public and private certificate authorities, session managers, policy entities, accounting and banking modules. The purpose of this architecture is to facilitate the delivery of secured information services offered at the roadside infrastructure.*

Keywords: *wireless vehicular networks, service provisioning, service sighting, security*

1. Introduction

Today, wireless communications have made possible the use of Internet-based applications such as web services, and technologies such as cellular networks, GPS-enabled devices, Wi-Fi and 3G. Direct Short Range Communication (DSRC) is a wireless admission technology based on the standard IEEE 802.11p and which is designed to handle different types of service applications, including the transmission of both safety and non-safety messages into two modalities: vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). DSRC is allocated at the 5.9 GHz frequency band and is designed to support high vehicular velocities in a radio transmission range up to 1000 m with a data rate up to 27 Mbps [1] per channel including two control channels and seven service channels.

The deployment of roadside antennas distributed along highways and roads covering extensive urban and rural areas, this type of infrastructure is intended for the use of public transport communication where the network infrastructure is constantly monitored by central network operation centers. One of the most important challenges in wireless communications deals with information security among communicating parties, especially in the case of vehicular ad hoc networks (VANETs) due to the dynamic behavior of vehicles.

In VANETs, there are different proposals concerning security in order to moderate the potential risks of attacks given that vehicles can have anonymous characteristics. For instance, a detailed description of different threats of attacks can be found in [2; 3; 4]; and [5] and a perspective on attack modeling in some vehicular scenarios is presented in [6].

In a vehicle-to-vehicle communication scenario, a major concern is the addition of false information by manipulating position, speed parameters or even identities. Moreover, as described in [7] denial of service (DoS) attacks can be caused by jamming the radio channel at the link layer or/and by saturating the vehicles forwarding capacity at the network layer. As a result of the risks imposed by network attacks, diverse types of proposals for authenticating and securing data have been proposed in order to provide reliable communications in VANETs such as in [11;13]. This paper describes a secure service architecture based on the presence of key modules which provide temporary session parameters for on-demand services intended for vehicular to infrastructure communications.

2. Communication Service Models

In general, Authentication, Authorization and Accounting (AAA) schemes [8] are intended to grant network and service admission to potential users only if specific admission policies and regulations are fulfilled by current requesters. Admission control mechanisms will promote the development of reliable and robust information services architectures in extended communication systems. Significant challenges concerning the support of scalable service provisioning models arise in highly mobile environments due to the presence of major constraints on the implementation of viable service models; such as the number of network elements in dense areas and the complexity of building stable network topologies.

In a service model perspective, it is possible to classify two main strategies offered on the road:

i. A compulsory subscription

ii. An on-demand service registration.

In the compulsory service subscription scheme, the user is required to register in advance to the provider's records in a commonly off-line environment; and then be subjected to authentication and admission control during a service request event. The latter establish a connection to an authentication server by using an AAA protocol to verify the user's credentials, i.e. the implementation of extensible authentication protocol (EAP) at the link layer and RADIUS protocol deployed at the network layer [9].

For on-demand service schemes, it is possible to consider that the provider has poor or even no knowledge of transitory requesters. For example, some on-demand requests can be visualized in scenarios where the roadside infrastructure advertises information services to potential users from specific content providers. This can be the case of navigation assistance services. In many situations, on-demand services can be considered as open service architectures eventually to all drivers who travel in the proximity; however, exchanges of information between users and providers must be kept reliable and secure, especially, when sensitive information is exchanged such as financial transactions or disclosure of user identities.

One advantage of the on-demand service modality is that under certain circumstances it will not rely in the use of extensive data storage infrastructure given the temporary behavior of vehicles since users are likely to be considered as "transitory" requesters. Therefore, the ability of the user to request network admission and services shall not be dependant to any specific admission infrastructure allowing users to request network and service admission regardless of their geographic location. An issue may arises when financial transactions take place, especially, when strict regulations must be complied and consistent records must be maintained concerning the transactions performed by customers.

A. Service sighting in Wireless Admission in Vehicular Environments (WAVE)

Information related to specific providers and corresponding channels are contained in a frame 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. The process to allow applications from a provider to be registered at the WAVE management entity (WME) consist of disclosing information such as channel of operation, address information, description of the services being offered and application priority.

Once the application is successfully registered at the local PST, then it is ready to be advertised through the roadside infrastructure. In order to guarantee the certainty of the information being transmitted the WSA frame is digitally signed and validated. In order to identify among different applications available at the local infrastructure, identifiers are required 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 user can distinguish and choose specific services contained in the PST.

3. Secure Service Architecture

The service architecture within the fixed network on which main elements provide reliability and profitability to the communication system is described in this session. The entire region is divided into service district domain as shown in figure 1. This service district is a logical zone that is usually mapped to a geographical zone where a set of services from different roadside providers are offered. All the modules contained within the administrative control of the district service entity are logically interconnected between them. Admission routers are illustrated as part of the core network but their main function is to provide connectivity to roadside units corresponding to specific wireless admission technologies.

Additionally, admission routers connect a set of registered information service providers residing at the fixed network. The interface between the district domain architecture and the core network is represented by an admission server.

User authentication is performed at the security module within the district administrative domain which can comprise the presence of multiple certificate authorities and/or their corresponding proxy modules. In the proposed architecture, the authentication of requesters is guaranteed by providing security features during the initial communication setup between users and providers. Certificate authorities (CA) are responsible for distributing and managing certified cryptographic keys between communicating parties. Moreover, CAs are responsible for keeping control of disclosed key certificates and the associated vehicle identifiers.

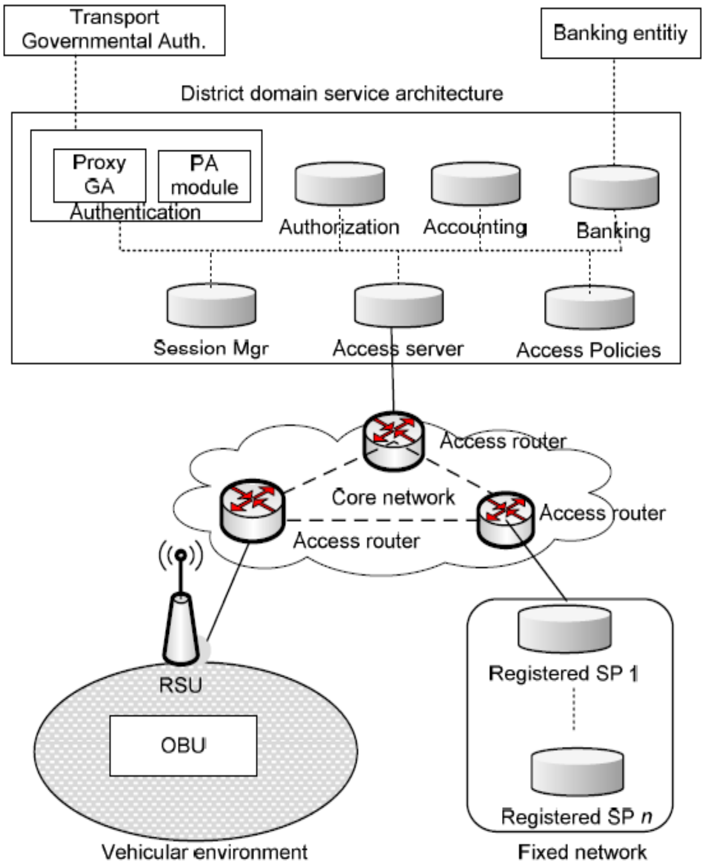

Figure 1. *Secure service architectural elements*

In the proposed architecture, we rely on the implementation of a PKI model involving both governmental authorities and private certificate authorities. In the following we describe in more detail the main elements comprising the security module.

Governmental authorities (GA): It is possible to consider the type of key provisioning by GA as permanent or semi permanent depending on governmental policies and regulations. This control might allow an official authority to identify the real identity of vehicles under certain situations. In [11], it is proposed that regional governmental authorities and possibly car manufacturers be in charge of registration operations; and that once the security material is available, it is preloaded in tamper-proof devices within vehicles [11;12;13]. In essence, in the proposed architecture, the certified key pairs provided by GAs 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 execution of strict control and registration procedures applied by official transport authorities to all vehicles and roadside units, as well.

Private Trusted authorities (PA): Based on a commerce premise, we might think in terms of fixed infrastructures which involve the partaking of heterogeneous applications from different service providers. For this reason, it is not suitable to consider the set of key certificates associated to a vehicle to be preloaded in advance before contacting a specific service provider [14]. Such a scenario would in fact mean that a user must previously store the public key for every provider he would like to contact. In the proposed architecture, the *PA* represents certified entities in charge of providing key distribution and key management mainly for on-demand requesters. The difference between *GA* and *PA* relies in that the latter issues temporary key certificates valid only during the service session. This means that every time a user requests admission to a service, new session keys are assigned for that specific session. Certainly, active collaboration between the *GA* and *PA* legitimate all communicating parties. Notice that in our architecture we include a secure proxy GA which serves as a proxy entity from an official transport authority for contact purposes. In the proposed architecture some assumptions have been considered. First, the security module must be capable to support and classify different types of requests depending on their priority and/or delay susceptibility. For some situations, the security module must rely just on the validation of the disclosed certificates by the requester without generating any kind of temporary cryptographic keying material. Second, commercial on-demand services might require the generation of temporary cryptographic keying material in order to support secure content delivery. Authentication of the public key certificates disclosed by requesters is carried on the validation of the non-revocation state (certainty) of those certificates via a certificate revocation list (CRL) [15]. Notice that authentication is based on the certainty of the current requester's certificates and not by user-id/password based authentication. Now, to secure the content of the new temporary cryptographic material (session key and session seeds/identifiers) generated by the *PA*, some main tasks must be considered.

1. Generation of *Ksession* session key, PA's certificate and signature (SIG), i.e. $Cert_{PA}\ \{PK_{PA}, SIG_{Priv/PA}\ (PK_{PA})\}$, where PK_{PA} is the *PA*'s public key and $Priv_{PA}$ is *PA*'s private key

2. Seeds or temporary identifiers are generated by the *PA* as SID_1 for the user and SID_2 for the corresponding service provider. These session seeds will serve as temporary user identifiers valid only for the session.

3. Encryption of the dispatched security attributes for the user by using the user's public key (K_{user}) which includes the new seed/identifier, token and session key, i.e. $Enc_{Kuser}[SID_1, token, Ksession]$.

4. Encryption of the dispatched security attributes for the provider by using a shared secret key ($K_{PA\text{-}SP}$) between the *PA* and the provider which includes the new seed/identifier, token and session key, i.e. $Enc_{PA\text{-}SP}[SID_2, token, Ksession]$.

5. The *PA* builds associations between the user's public key certificate, the new session seed (SID_1), tokens and common session key.

6. The *PA* builds associations between the provider's public key, the new seed (SID_2), tokens and common session key.

After the authentication phase has been explained, it is worth to emphasize the importance of sorting the type of service which can be delivered by the roadside infrastructure. Service policies are contained at the policy module and which define the way information must be handled. From the vehicle perspective, there might some situations where safety-related messages or sensitive-delay data must be treated as fast as possible; so a service taxonomy can allow that safety-related messages might be tagged with a higher priority compared to that intended for commercial services.

In general, any of exchange of information related to the execution of financial transactions must be collected and analyzed at the banking module. From the district domain, banking entities 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, as well as, for defining banking regulations and the related cost consumption policies. We assume that there must be a pre-established relationship between the banking entity and the user for validation purposes which can be based either on user identifiers or some special type of banking credentials. This kind of banking validation resembles a credit-card payment modality where the ability of the user to acquire 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 potential communicating parties has been successfully completed; that is, when session keys are available for the provider who intends to deliver the service and the requesting user. Once a successful validation of the user takes place, then the banking entity is able to dispatch the corresponding credit units and a transaction identifier which can specify the amount of content data to be retrieved or the maximum time duration for the service session.

At the accounting module, temporary registers are created to keep track of transitory users containing the temporary user identifier (seed), session identifier, credit units, tokens, transaction identifier, provider identifier, service identifier and expiration session time. Moreover, the accounting module contains specific policies which define the way temporary registers are maintained and updated. The authorization module grants resource assignation when validations at the previous modules have been completed. Regarding the presence of the session manager, its main function is to retrieve information from the accounting module and 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 is performed through the interaction of current participating session managers. These entities can be considered as the final stage in the response process and which task is to assemble all the parameters created for a specific service request before sending back the secure attributes to the corresponding parties.

A. Collaboration in Multi-Hop Environments

In the special case of VANETs, we focus on the distribution of incentive units along the multi-hop path such as some incentive approaches proposed in [16;17]. Incentive must be required when messages have to be propagated beyond the radio transmission range in order to reach the destination. Here, we make an assumption that a routing protocol exists and is operational among vehicles. Basically, at the secure service architecture the validation and generation of security attributes for the corresponding user and the SP follows the same procedure as in a single user case. The difference relies in the ad hoc environment where sensitive information is encrypted at the authentication phase by using the secret key between the user and the PA. For the payload delivery phase, the information is encrypted by using the temporary session key between the user and the SP. In either case, there is no chance for intermediate nodes to extract the contents of the transmitted message since they do not have the corresponding keys to decipher the messages.

Then, the main tasks to be performed by intermediate nodes are to validate the preceding sender's signature by using the corresponding neighbor's public key certificate and to forward the packet with the current node's signature. Based on the forwarding path followed during the initial authentication process, banking entities can provide bonus units along with tokens for those nodes participating in the forwarding path. These incentive units promote active participation of neighboring nodes and can serve as cumulative benefits for later rewards. Some w kind of incentive is necessary as local resources are utilized at every single forwarding node in order to deliver the payload messages up to the final user. Along the path,

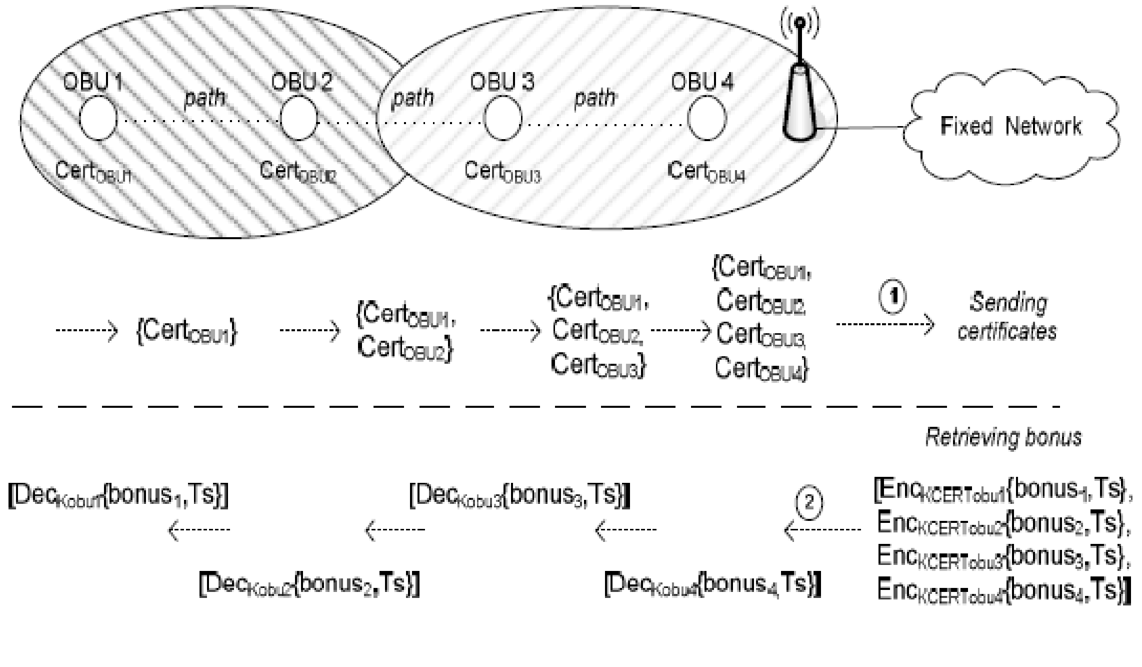

Figure 2. *Distribution of bonus units in multi-hop scenario*

e consider that a chain of certificates must be built through public key certificates for every single intermediate node (see figure 2).

At the banking entity, there is an association between a bonus unit and its corresponding public key certificate which also serves to encrypt the dispatched bonus units and respective tokens. Consequently, at every forwarding node, the current node will be able to decrypt the bonus unit by using the corresponding private key. The following list summarizes the above procedure.

1. Intermediate node$_i$ sends public key certificate $Cert_{OBUi}$.

2. Token (Ts) and th bonus unit are encrypted with node$_i$ public key certificate, $Enck_{certOBUi}\{bonus_i, T_s\}$

3. At intermediate nodei, message is decrypted with node$_i$'s private key, $Decky_{OBUi}\{bonus_i, T_s\}$.

Additionally, each node must have a specific buffer to store all received bonus units. However, there is an open issue to solve in the way that what if the *n*-node accepts the bonus unit but it fails to deliver payload packets. For now, we assume that the delivery of packets through the intermediate *n* node is guaranteed. Clearly, this assumption possesses the risk of getting bonus units without participating in the packet delivery. For the ad hoc environment, some possible solutions can be suggested as the deployment of reputation systems such as watchdog [17;18] which is in charge of monitoring the forwarding behavior of every single node in the delivery path. If an intermediate node fails trustworthiness, this node is discarded from the forwarding path. In summary, the exchange of service messages is secured at every forwarding point. This procedure can guarantee that the message is legitimated by the participating intermediate nodes along the path from the user to the SP. Furthermore, this scheme promotes collaboration between nodes through the use of incentives issued at the fixed infrastructure.

4. Conclusion

In this paper, relevant characteristics about service provisioning and admission architecture in a vehicular context have been presented. The major concern in vehicular network is the need to provide service sighting and secure admission to services where reliable delivery of information between vehicles and providers must be guaranteed. We propose a secure service admission architecture based on the concept of district domains which are entities responsible for dispatching session parameters to on-demand users within an administrative domain. The service architecture comprises the presence of public and private certificate authorities, session managers, policy entities, 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 session key for both the requesting user and the solicited provider. Regarding the policy module, it is in charge of defining service policies and regulations. At the banking module, a validation takes place in order to certify that the user's baking credentials can afford the requested service. The accounting module will generate a temporary record concerning all the service parameters associated to the transitory user. The authorization module grants resource assignation when validations at the previous modules have been completed. One of the main parts of this architecture 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. Finally, future research work might be oriented to tackle highly dynamic trajectory patterns in ad hoc networks, especially when a large number of vehicles are involved and their trajectory patterns become unpredictable.

References

[1] DOT HS 809 859 nhtsa. Vehicle Safety Communications Project Task 3 Final Report. Identify Intelligent Vehicle Safety Applications Enabled by DSRC. March, 2005.

[2] Papadimitratos, P., Kung, A., Hubaux, J. and Kargl, F. "Privacy and Identity Management for Vehicular Communication System". eSafety, 2005.

[3] Capkun S., Hubaux, J. and Jakobsson M. 'Secure and Privacy- Preserving Communication in Hybrid Ad Hoc Networks'. EPFL-IC Technical Report, 2004.

[4] Mishra, A. and Nadkarni, K. "Security in Wireless Ad Hoc Networks". The Handbook of Wireless Networks, Chap. 3. M. Ilyas, 2003.

[5] Zhou, D. "Security Issues in Ad Hoc Networks". The Handbook of Wireless Networks, Chap. 32. M. Ilyas, 2003.

[6] Aijaz, A., Bochow, B. and Dotzer, F. “Attacks on Inter Vehicle Communication Systems – an Analysis”. 3rd International Workshop on Intelligent Transportation (WIT 2006), March, 2006.

[7] Blum J. and Eskandarian, A. “The Threat of Intelligent Collisions”. IT Pro, IEEE Computer Society, Feb. 2004.

[8] Housley, R. and Aboba, B. RFC 4962, ‘Guidance for Authentication, Authorization and Accounting (AAA) Key Management’, Network Working Group, IETF Trust, 2007.

[9] Atwood, W. ‘An Architecture for Secure and Accountable Multicasting’. 32nd IEEE Local Computer Networks, Ireland, 2007.

[10] IEEE Trial-Use Standard for Wireless Admission in Vehicular Environments (WAVE)-Networking Services. IEEE Std 1609.3™- 2007.

[11] Raya, M., Papadimitratos, P. and Hubaux, J. ‘Securing Vehicular Communications’. EPFL, 2006.

[12] Raya, M. and Hubaux, J. ‘The Security of Vanet’. ACM SASN’05, USA. 2005.

[13] Dotzer, F. ‘Privacy Issues in Vanet’. Workshop on Privacy Enhancing Technologies, Croatia, 2005.

[14] Coronado, E. and Cherkaoui, S. ‘Secure service provisioning in vehicular networks’, UBIROADS’07, Morocco, 2007.

[15] Housley, R., Polk, W., Ford, W. and Solo, D. RFC 3280. ‘Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile’. Network Working Group. Internet Society, 2002.

[16] Buttyan, L. and Hubaux, J. ‘Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks’. Kluwer. Mobile Networks and applications 8, pag. 579-595, 2003.

[17] Buttyan, L. and Hubaux, J. ‘Enforcing Service Availability in Mobile Ad-Hoc WANs’. EPFL-DSC-ICA, 2000.

[18] Fonseca, E. and Festag, A. ‘A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETs’. NEC Network Laboratories, 2006.

[19] Obreiter, P., Koning, B. and Klein, M. ‘Stimulating Cooperative Behavior of Autonomous Devices’. 2nd International Workshop on Wireless Information Systems (WIS2003), France, April 2003.