DISTRIBUTED CERTIFICATE AND APPLICATION ARCHITECTURE FOR VANETs

Baber Aslam and Cliff Zou
University of Central Florida
Orlando, FL

ABSTRACT

Privacy, authentication, confidentiality and non repudiation are the most desired security attributes for all vehicular ad hoc network (VANET) applications. A lot of solutions have been presented to address these issues. However, they are mostly dependent on centralized certificate architecture and some sort of hardware-based security. These solutions are expensive to carry out and lack the incentive for both users and service providers to deploy, which make them especially difficult to be implemented during the important initial deployment stage of VANET.

In this paper, we present a distributed security architecture for VANET that does not rest on expensive security hardware or elaborate security infrastructure. The architecture can be incrementally deployed, facilitating small companies to jump in the VANET business, and can fill the void during the VANET initial deployment phase. Our solution is based on spatial and temporal restricted certificates, which are issued upon user's request and can be used for various VANET applications. Due to the restricted nature of these certificates, the certificate revocation process is simple and efficient, which solves another drawback of existing solutions.

1. INTRODUCTION

All VANET applications either collect or disseminate information from/to vehicles. The authenticity of the information is very important since malicious information may result in loss of life and property. This authenticity of information can be achieved, if some means of liability are introduced. Besides non repudiation; confidentiality, privacy and authentication are the desired security attributes. The best possible solution is to use digital certificates issued to (tied to) a user/provider by a trusted third party. These certificates can then be used to sign the information. Most of the existing solutions use some kind of certificates with a central certificate-issuing/trusted authority [1-7]. The architecture successfully achieves authentication, confidentiality and non repudiation but compromises the privacy since the signed information can be linked to the signer. To provide privacy, the architecture can be extended to use many temporary certificates (or called pseudonyms) instead of one permanent certificate [2, 3]. These pseudonyms can be preloaded in a tamper proof device - TPD [2], issued by an online authority [1, 3] or generated by user himself [4, 5].

The centralized certificate authority (CA) based solutions present a number of challenges which may be difficult to address during the initial deployment stages of VANET. The CAs must be organized in a hierarchical manner for effective management. The hierarchy can be area/location based; a given area (e.g., United States or Europe) can be divided into regions (e.g., states or countries) with each region having its regional CA, these regional CAs are then linked with each other via a top level CA. Figure 1 shows a hierarchy with two regions.

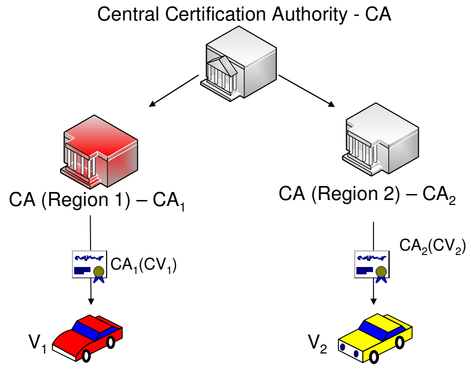

Figure 1. A certification authority hierarchy with two regional CAs. CA (Region 1) issues certificates to vehicles registered with in its region, for example certificate CV$_1$ is issued to vehicle V$_1$. (Note: CA$_x$(CV$_y$) is a certificate issued to vehicle y by a CA of region x.)

The hierarchy can be extended both upwards and downwards. This means for vehicles to easily travel outside their CA's domain, we need to establish a trust relationship among all certification authorities; thus certificate verification may take longer if the trust relationship goes through a long chain. Figure 2 shows possible steps taken for certificate verification when a vehicle from one region tries to communicate with a vehicle from another region (it assumed that none of the intermediate entities have previously cached certificates).

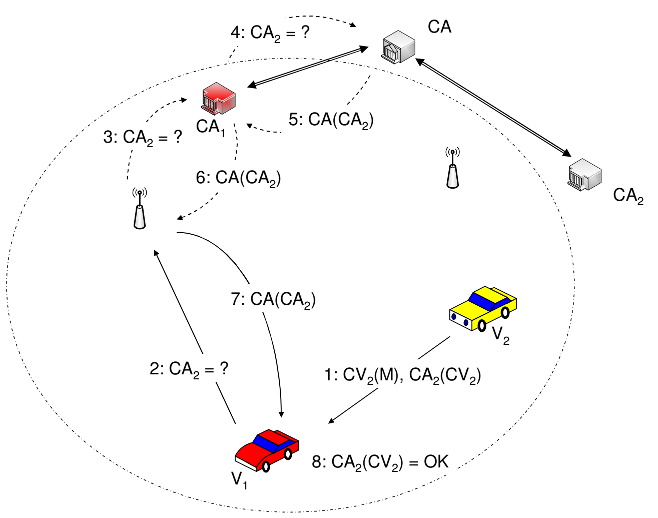

Figure 2. Certificate verification. (1) V_2 sends a signed message along with its certificate to V_1. V_1 does not have certificate CA_2 in its cache and therefore cannot verify CV_2. (2, 3) V_1 asks for CA_2 from its regional CA via roadside unit. (4) Regional CA may have to ask central CA for the CA_2. (5, 6, 7) Certificate $CA(CA_2)$ is sent to V_1 via regional CA and roadside unit. (8) V_1 verifies the certificate CA_2/CV_2 and accepts the message. (Note: $CA_x(CV_y)$ is a certificate issued to vehicle y by a CA of region x and dotted circle indicates a region.)

Further, it also makes revocation difficult since revocation list (RL) must be distributed to all regions as vehicles are not restricted to remain within their regions. Figure 3 shows the distribution of RL in case of two regional CAs. If pseudonyms are preloaded in TPDs then certificate revocation for a particular vehicle must include all the pseudonyms currently issued to (stored in) the vehicle. The RL may grow over time, making its distribution more difficult.

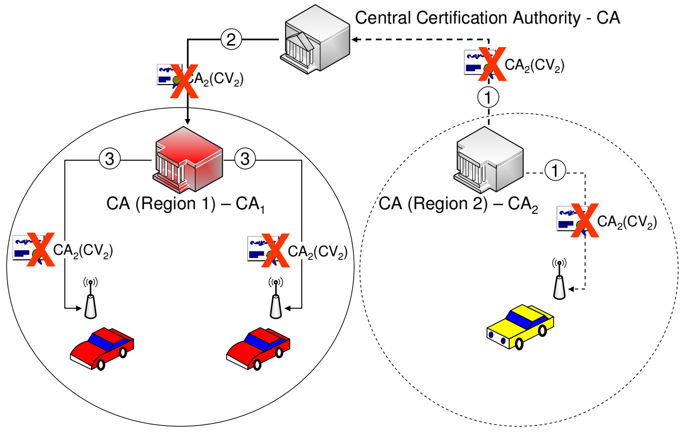

Figure 3. Distribution of certificate revocation list. (1) CA (Region 2) revokes certificate of a vehicle in its region, it distributes the revocation information within its region and also forwards it to central CA. (2) Central CA forwards revocation information to all regional CAs. (3) Each regional CA disseminates revocation information within its region. (Note: $CA_x(CV_y)$ is a certificate issued to vehicle y by a CA of region x and circles indicate regions.)

Each vehicle will have an associated certificate since its manufacture, this will be modified or updated each time the owner changes. These certificates will be expensive and it will also be technically difficult for an average user to keep track of the certificate renewal etc (even if he is not using the services). Further, in case of possible compromise, the revocation and issuance of new certificate may be quite cumbersome.

In current designs, too much trust is placed on TPD, which stores all cryptographic materials (permanent certificate and pseudonyms), performs cryptographic operations (signing/verifying messages) and processes revocation messages/commands (erase keys/pseudonyms when revoked) [2]. Since the vehicle (and TPD) cannot be physically guarded as other electronic security devices (smart cards etc), those requirements will make the device quite expensive [8]. Further, the pseudonyms when exhausted must be reloaded thus requiring a periodic maintenance.

The initial deployment stage of VANET will be characterized by limited infrastructure and small number of smart vehicles, which means very limited vehicle to vehicle and vehicle to infrastructure communication. During this stage, the solutions that assume omnipresence of these communications for certificate issuance, verification or revocation will not be practicable. Further, lack of infrastructure will discourage consumers' participation and lack of consumers (smart vehicles) will discourage providers' investment in infrastructure.

To address these challenges, we propose a distributed certificate architecture. Certificates with a limited scope in both time and space domain are issued by a service provider. These certificates are usable within a particular geographic area or within a certain time or both. These certificates are not tied to the vehicle's registration etc and can be changed periodically during one service period. Meanwhile law enforcement agencies can trace back the user via the temporary certificate and the service provider.

The paper is organized in five sections. Section two discusses the related research, section three explains the proposed solution, four presents analysis of the proposed solution, and section five gives conclusions/future work.

2. RELATED WORK

IEEE P1609.2 [1] proposes a CA based architecture; it also uses pseudonyms for privacy. These pseudonyms are short lived and are issued on vehicles request. This architecture assumed pervasive roadside architecture and also does not offer certificate revocation options.

Papadimitratos et al. [2, 3, 9] have presented a quite comprehensive solution based on central/regional certification authorities and their trust relationships. The solution uses pseudonyms to address privacy issues. The pseudonyms are preloaded in TPD [2] or issued by pseudonym provider [3] or generated by TPD and signed by CA [9]. They have also highlighted multiple revocation protocols. The solution requires the TPD, of the vehicle whose certificates have been revoked, to delete all stored pseudonyms and also assumes CA to have some knowledge about vehicles location. A malicious node may avoid this deletion by blocking the revocation message. This may enable him to use the pseudonyms later for communication with other vehicles. Other options are distribution of compressed RL or using bloom filters. TPD management through signed messages from CA may be exploited to evade revocation or for other malicious purposes such as DoS attacks (causing victim's TPD to delete key material, etc). [9] leaves misbehavior detection on vehicle between infrequent RL distributions.

The distribution of RL to all smart vehicle/regions is also a challenge. Papadimitratos et al. suggest restricting the scope of RL within a region, and requiring visiting nodes from other regions to obtain temporary certificates [10]. Thus a vehicle will have to acquire temporary certificates if it is travelling outside its registered region.

In [11] Parno et al. present detailed discussion on challenges faced by vehicular network, adversaries, attacks and propose a set of security primitives. They suggest a dynamic key distribution system, where each node generates its own short term key pair and requests CA to issue a certificate based on generated public key. They also suggest using group signatures to achieve anonymity.

In [4] Armknecht et al. propose a public key infrastructure where users derive public keys, certificates and pseudonyms. The architecture is based on elliptic curves, each user gets a master key and master certificate from CA. It can then generate its key pairs or certificate using masker key, master certificate and its own secret key. The certificate generated by user is verifiable by CA's public key. For revocation the CA publishes some data depending on which all nodes have to update their keys. The excluded nodes cannot update the keys based on this data. This means for each revocation everybody has to update their certificates.

In [5] Fan et al. present detailed operation of public key infrastructure mechanism based on bilinear mapping. They achieve privacy through pseudonyms which are generated by users themselves similar to [4]. Revocation is accomplished through distribution of RL that is stored by each user stores. Every time a user receives a beacon it performs certain computations on complete RL to ensure that the received beacon is from unrevoked user.

In [12] Lin et al. present a security mechanism using group signature and identity based signature techniques. The solution minimizes the storage at CA for later liability establishment, however the revocation is road side unit aided. CA sends RL to roadside unit which then monitors certificates in messages broadcasted by passing-by vehicles and if a message with revoked certificate is observed then roadside unit broadcasts warning messages. In another option it is suggested that each passing-by vehicle get its certificate signed from roadside unit. These signatures are then used to show that the certificate has not been revoked. First option is open to attacks (malicious node does not transmit within range of a roadside unit) and second increases complexity and overhead.

Our solution is also based on certificates to achieve desired security attributes, but it differs in a number of ways from solutions presented above. We do not require expensive TPD preloaded with pseudonyms or an elaborate/centralized public key infrastructure. Our solution does not have a lengthy certificate verification process and also does not require vehicles to recertify their certificates when travelling outside their parent region. The solution does not have a complex certificate revocation procedure, further, our solution does not suffer from RL distribution issues such as revocation evasion by malicious nodes or delayed RL distribution. We present a distributed certificate architecture where certificates are time and space restricted. The architecture simplifies certificate issuance, renewal and revocation processes without requiring expensive hardware or infrastructure.

3. PROPOSED SOLUTION

In this paper our focus is to achieve the desired security attributes (Privacy, authentication, confidentiality and non repudiation) during the initial deployment phase of VANET. This phase will be characterized by very few smart vehicles and lack of necessary roadside infrastructure to support various VANET applications or elaborate security architecture. We propose an architecture that achieves desired security attributes and enables service providers to offer incrementally various VANET services with minimal investment thus encourages both service providers and users to try/adopt VANET.

3.1 Assumptions

Our solution is based on a few simple assumptions given below:

- The user/node (we use user/node/vehicle interchangeably in this paper) has a payment-processing-device (similar to automatic toll payment devices - sold for tens of dollars). We do not require the device to store pseudonyms, perform cryptographic operations (such as signing/verifying messages) or perform revocation operation. The device only participates in credential/service request operations (discussed later).
- The user/node has a wireless-communication/VANET-application device that can communicate with roadside infrastructure; it can be a laptop or a hand-held device or a device specially designed for smart vehicles. The device can communicate (wired/wireless/WiFi/Bluetooth) with the payment-processing-device.
- Limited local roadside units are available (the existing hotspots in urban areas may be used for this purpose) and service providers can be accessed through these roadside units.

3.2 Basic Solution

The basic solution only caters for the provision of temporary credentials so that the required security attributes are achieved. These temporary credentials (pseudonyms) can then be used for basic vehicle to vehicle communication or participation in VANET safety application (such as initiating/relaying safety information).

The basic idea is that if a user wants to participate in a VANET (the user's vehicle is not required to have a manufacturer's issued certificate), he purchases a payment-processing-device (As mentioned above, it is assumed that user also has a VANET application device, which is running desired VANET applications). Each device will have an identification and an associated certificate. During initialization the device will be linked/registered with the user's account. The user's information will be maintained with the provider and will not be stored in the device. The basic procedure is illustrated in Figure 4. When a user enters a service area and wants to use the service, he makes the payment for the service using onboard payment device. The payment-authorization/service-request message will be encrypted using the provider's public key, thus hiding the device ID/certificate and services requested from eavesdroppers. The user is issued a pseudonym by the provider that will be valid for a given period/area.

We define several notations/functions that we will use in the formal description of our solution. A certificate or a pseudonym will essentially be represented by its public and private key pair; such as (K_x^+, K_x^-) are public (+) and private (-) keys belonging to *X*. (t_s, t_f) are the start and finish times between which a particular pseudonym (*P*) will be valid. A certificate can be valid inside a service area; service areas can be defined with region numbers *R*, large service areas may have more than one region. A user specifies the region and time period, in the request, for which he/she wants to purchase the certificate. $E_{K^+}(M)$ defines an encryption function on message *M* using the public key K^+. Public cryptography is very resource intensive therefore data encryption is usually carried out using a randomly generated symmetric session key and only the session key is encrypted using public cryptography. The encryption function $E_{K^+}(M)$ defined above employs similar techniques; we will not show the details for simplicity and compactness. $S_{K^-}(M) = N$, defines a signature function on message *M* using a private key K^-. The signatures are computed by first creating a message digest using a hashing function and then encrypting the digest using key K^-. $V_{K^+}(M, N)$ is a signature verification function. It has two inputs the message *M* and the signature *N*. It verifies the signature by computing the message digest of message *M* and comparing it with received signatures *N* (after decrypting it with the corresponding public key K^+).

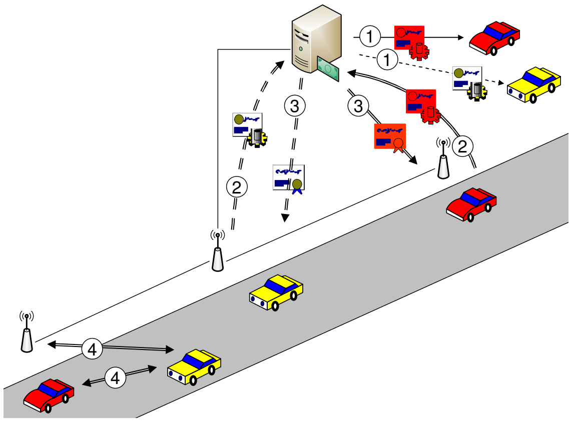

Figure 4. Architecture (1) Users register their payment devices with Provider beforehand (2) Users send payment/service requests (3) Provider issues temporary credentials (4) Users participate in VANET via vehicle to vehicle or vehicle to infrastructure communication.

If a user *U* having a public key pair (K_U^+, K_U^-) (for initial request these are the permanent keys associated with the payment-processing device) wants to acquire temporary credentials for the time duration defined by (t_s, t_f) and within the region *R* from a service provider *S* with a public key pair (K_S^+, K_S^-), figure 5 shows the transactions.

```
1  $U:$         Generate $M = \{t_s, t_f, R, U\}$
                Compute $M_R = E_{K_S^+}(M)$
                Compute $N_R = S_{K_U^-}(M)$
2  $U \rightarrow S:$  $M_R, N_R$
3  $S:$         Extract $M$
                $V_{K_U^+}(M, N_R)$ [a]
                Verify ID $U$ and associated account
                Generate $P = \{t_s, t_f, R, K_P^+\}, K_P^-$ [b]
                Compute $M_P = E_{K_U^+}(P, K_P^-)$
                Compute $N_P = S_{K_S^-}(P)$
                Compute $N_K = S_{K_S^-}(K_P^-)$
4  $S \rightarrow U:$  $M_P, N_P, N_K$
5  $S:$         Extract $P$ and $K_P^-$
                $V_{K_S^+}(P, N_P)$, $V_{K_S^+}(K_P^-, N_K)$
```

[a] The service provider records device's public key during user/device registration/initialization process.

[b] P is the pseudonym/temporary certificate with associated private key K_P^-

Figure 5. Transactions between User *U* and Provider *S* to acquire temporary credential $\{t_s, t_f, R, K_P^-, K_P^+\}$***;*** **valid for time duration defined by** (t_s, t_f) **and within region *R*. User uses *(P, N_P)* as a temporary certificate.**

3.3 Extended Services

The solution can be easily extended for extended/additional services. If additional VANET services or applications are available (such as multimedia content, web access, email etc) then these can be offered as extended services. In this case a user indicates the service which he desires to use/purchase in service request/payment authorization message. The payment processing provider issues the temporary credentials to the user and also forwards these credentials along with the details of service purchased to the concerned server. The user can then initiate request to the concerned server for service using issued temporary credentials. Figure 6 shows such a scenario. The Extended services will include the basic service (basic service only provides pseudonym).

It is not necessary that the payment-processing provider is also operating the application servers; these servers can be operated by other providers. In this case, the payment-processing provider provides temporary credentials and processes the payments on behalf of other providers; similar to credit card providers.

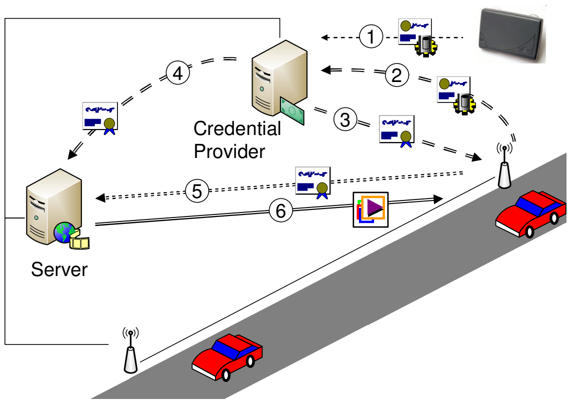

Figure 6. Extended services architecture (1) User registers payment device with Credential provider (2) User sends payment/service request (3) Credential provider issues temporary credentials (4) Credential provider informs Server of service purchased and temporary credentials (5) User requests service using temporary credentials (6) Server delivers content.

3.4 Provision of Privacy

The privacy is one of the most important security attributes in VANET. The proposed solution provides this through pseudonyms which cannot be linked to the user ID. For additional privacy the pseudonyms can be refreshed within one service period. There are two possible options for this; the pseudonyms are issued in bulk at the time of purchase or a new pseudonym is issued sometime before the expiry of the old pseudonym.

In case of bulk issuance of pseudonyms there are a few aspects to be considered. The number of pseudonyms is related to time period for which the service has been purchased and desired level of privacy (i.e. how often the pseudonyms are changed). (In this paper we are not considering the exact time period or methodology for changing pseudonyms; this has been studied in detail by other researchers [9, 13-15, 18].). The validity period of each pseudonym is also important. If multiple pseudonyms have overlapping validity periods, they may be used for Sybil attacks. Although each pseudonym can be traced back to the user via a payment-processing-provider, this can only be done by law enforcement/government agencies and not by ordinary users. Another important aspect is the length and number of messages that are required to send these pseudonyms to the user/server and also the storage requirement at server/user device. If the pseudonyms are sent in one or multiple continuous messages, a malicious server (not the credential provider) may be able to link the pseudonyms and compromise user's privacy. For this reason, the credential provider should first mix/group the pseudonyms of different users (that will be served by same server) with each other and then send them to a service provider. User's applications also need to be careful about changing the pseudonyms to ensure security and uninterrupted service, for example not changing a pseudonym within a transaction or between multiple transactions that can be linked based on context (accessing one's email).

In case of single issuance of pseudonym the most important aspect is to ensure that the user gets new pseudonym before the expiry of current one. There are two options for this, either the user initiates request for a new pseudonym before the expiry of current one or the server maintains state for each user and issues a new pseudonym before the expiry of current pseudonym. Letting users initiate requests is more practicable since it will save server's resources and the complexity of message delivery (the user can initiate request anywhere within the service area).

Besides certificates (pseudonym) other IDs (such as IP address, MAC address etc) are also important to hide in ensuring privacy [16, 17]. These IDs can be issued on temporary basis and refreshed several times during a service period similar to pseudonyms.

The certificate of CA (also the payment-processing-provider) is hard coded in the payment device, enabling other users to check the validity of a certificate.

3.5 Practicability

The proposed solution is incremental, practicable and requires minimal infrastructure, which is especially advantageous during the initial deployment phase of VANET. The payment-processing-device does not need to have many functionalities or high processing power or large storage. It is similar to toll-payment-devices which are commonly being used and can be purchased for tens of dollars.

The payment-processing-device is not tied to a particular vehicle so a user is free to transfer it from one vehicle to another. The payment-processing provider is similar to credit card providers; we are using the mature Internet-like payment-processing architecture which is considered to be secure.

The application servers can be installed by different operators and existing hot spots in urban areas may be initially used to test the architecture.

Software can be developed for laptops and handheld devices to participate in different VANET applications. This will also provide a framework where different VANET applications can be tried or tested.

4. ANALYSIS

The proposed architecture ensures desired security attributes. Authentication and confidentiality can be achieved by signing/encrypting the messages using associated public keys. Attacker cannot link the pseudonyms with a user; even different pseudonyms cannot be linked with each other, thus ensuring privacy. Meanwhile, liability can be enforced with the help of payment processing provider, since it has the account information for each issued pseudonym.

The architecture, as opposed to existing solutions, does not require users to maintain permanent (long-term) or valid temporary certificates when they are not using the service; user purchases a certificate only when he wants to use the service. The architecture also simplifies the certificate revocation; certificates automatically expire after their validation time or beyond the predefined service area. For each new issuance of a certificate the provider checks if a previous certificate for the same user was revoked (each user account has an associated revocation flag that indicates whether a previous certificate of user was revoked or not. The provider can reset the flag if the user later clears the cause of revocation). If a revocation entry exists then new certificate will not be issued. Further, if the certificate is to be revoked before its expiry then revocation list (RL) can be disseminated via roadside units. Since the service is area/time restricted so the RL will be distributed only within the effected area and will contain only the certificates which have still not expired (due to time). This simplifies RL maintenance and distribution.

The system does not require centralized CA or trust relationships among regional CAs. Each provider can work independently within its coverage area. This minimizes the infrastructure required by a service provider to start its services and will be an incentive for service providers and facilitate small companies jumping into the VANET industry. Initially, a service provider may limit its service within a geographic area and later incrementally extend it. Further, when isolated/widely-separated service areas become adjacent due to the extensions then they can be combined as one region or roaming can be coordinated between the regions. Users and providers both benefit with incremental deployment without paying unnecessarily for the services they do not use or sell. The solution does not require expensive tamper proof devices and periodic refilling of pseudonyms. A user only pays when using the service and does not pay for certificate maintenance.

Payment devices may be operated by a third party and integrated with service providers; one device may be used by different service providers. Further, development of payment device will be motivated by service providers, who will force security and affordability of the devices. The architecture derives its security from the mature Internet payment systems.

As a baseline service, the temporary credentials can be used for all VANET applications including vehicle to vehicle communications. Further, our solution can coexist with the solutions that are based on the certificate authority and changing pseudonyms (such as [1-3, 9]), therefore smart vehicles equipped with TPDs and vehicles using our solution can coexist and make use of the service provided by the providers. This ensures smooth transition and unlimited overlapping of both solutions.

The certificates can be used for other cryptographic primitives, such as session keys between users, group keys within area for broadcast/multicast of a particular service etc. The solution can guard against Sybil attacks, since one payment processing device will be issued one certificate, if more than one payment device is used then it is possible, but the attacker has to pay for the Sybil node also.

5. CONCLUSION

We have presented a distributed certificate architecture that can be incrementally deployed. Users are issued with temporary certificates which can only be used within a specific geographic area and within a particular time period. This property also simplifies the certificate revocation procedure. We have also presented the framework which can be used to provide various services to VANET by providers without investing much in infrastructure. The solution is intended to stimulate people's interest in VANET and build user/provider confidence. In future work, we intend to extend the architecture to cater for later stages when isolated service areas become adjacent or overlap each other (due to their extensions). In this case we need to introduce some roaming or cross certification mechanisms between the service areas.

REFERENCES

[1] "IEEE P1609.2 trial-use Standard for Wireless Access in Vehicular Environments: Security Services for Applications and Management Messages," July 2006.

[2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," In IEEE Wireless Communications Magazine, pp 8-15, October 2006.

[3] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," In Proceedings of the 7th International Conference on ITS Telecommunication, June 2007.

[4] F. Armknecht, A. Festag, D. Westhoff, and K. Zang, "Cross-layer privacy enhancement and non-repudiation in vehicular communication", In Proceedings of the 4th Workshop on Mobile Ad-Hoc Networks (*WMAN'07*), March 2007.

[5] C. I. Fan, R. H. Hsu, and C. H. Tseng, "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network", In Proceedings of the International Conference on Mobile Technology, Applications and Systems, September 2008.

[6] G. D. Crescenzo, T. Zhang , and S. Pietrowicz, "Anonymity notions for public-key infrastructures in mobile vehicular networks", In Proceedings of the 4th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'07), October 2007.

[7] J. Choi and S. Jung, "A security framework with strong non-repudiation and privacy in VANETs", In Proceedings of the 6th Annual IEEE Consumer Communications & Networking Conference IEEE CCNC 2009, January 2009.

[8] A. Stampoulis and Z. Chai. Survey of security in vehicular networks, project CPSC 534, http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf, 2007, last access: May 14th , 2009.

[9] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: design and architecture", In IEEE Wireless Communication Magazine, November 2008.

[10] P. Papadimitratos, G. Mezzour, and J. P. Hubaux, "Certificate revocation list distribution in vehicular communication systems", In Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking VANET'08, September 2008.

[11] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", In Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV), November 2005.

[12] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, "Security in vehicular ad hoc networks", In IEEE Communication Magzine, pp 88-95, April 2008.

[13] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs", In Proceedings of the 3rd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, July 2007.

[14] A. R. Beresford and F. Stajano, "Mix Zones: User privacy in location-aware services", In Proceedings of the 1st IEEE International Workshop on Pervasive Computing and Communication Security (PerSec), March 2004.

[15] S. Eichler, "Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility", In Proceedings of the 2007 IEEE Intelligent Vehicles Symposium, June 2007.

[16] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis", Mobile Networks and Applications, v.10 n.3, p.315-325, June 2005.

[17] E. Fonseca, A. Festag, R. Baldessari and R. Aguiar, "Support of anonymity in VANETs – Putting pseudonymity into practice", In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), March 2007.

[18] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-PHubaux, "Mix-zones for location privacy in vehicular networks", In Proceedings of the 1st International Workshop on Wireless Networking for Intelligent Transportation Systems (Win-ITS), August 2007.