An Identity-Based Security Framework For VANETs

Pandurang Kamat *
pkamat@winlab.rutgers.edu
Wireless Information Network Laboratory (WINLAB)
Rutgers University, NJ.

Arati Baliga
aratib@cs.rutgers.edu
Department of Computer Science
Rutgers University, NJ.

Wade Trappe
trappe@winlab.rutgers.edu
Wireless Information Network Laboratory (WINLAB)
Rutgers University, NJ.

ABSTRACT

We present a security framework for Vehicular Ad hoc Networks (VANETs), using identity-based cryptography, to provide authentication, confidentiality, non-repudiation and message integrity. Additionally it provides scalable security and privacy using short-lived, authenticated and unforgeable, pseudonyms. This feature can be used by VANET applications that require quantifiable trust and privacy to provide differentiated service based on various levels of trust and privacy thresholds.

Categories and Subject Descriptors: D.4.6[Security and Protection]: Authentication

General Terms: Security.

Keywords: Security, Privacy, Vehicular networks.

1. INTRODUCTION

Researchers are continually exploring the feasibility of vehicular applications, ranging from enhancing driver safety to traffic management to providing roadside services and infotainment using inter-vehicle communications. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology.

Adversarial models for such communication networks range from mere eavesdropping to malicious data injection to cause accidents. Any security solution has to account for the contention-based opportunistic communication medium, transient association and ad-hoc group formations between vehicles, ease of eavesdropping and disrupting the message and data exchange, high mobility, and the acute need for privacy in these networks.

Vehicles and base-stations should be able to authenticate themselves and at the same time use disposable pseudonyms for vehicles so that their activities and communications are not tracked by parties that are eavesdropping on them. We also need to make certain that there is a verifiable trail between the pseudonyms and the real identities of the vehicle and that only a common, Trusted Arbiter(TA) is able to verify that trail in case of a dispute.

Proposed security solutions using traditional public key[5, 4] cryptography are not very flexible in providing user specified levels of privacy due to rigid pseudonym assignments nor bandwidth efficient because of the size of keys and certificates used. The solution, using symmetric keys, proposed in [3] is not suited to delay-sensitive vehicle-to-vehicle communication as vehicles have to contact a base station to decrypt/verify information given by another vehicle.

We propose a security framework for vehicular networks, using Identity-Based Cryptography (IBC), that provides authentication, confidentiality, message integrity, non repudiation and pseudonymity. We present a pseudonym generation mechanism that exploits the implicit authentication provided by IBC to generate unforgeable, authenticated pseudonyms. While these pseudonyms allow vehicles to engage in anonymous communication, they also provide non-repudiation because [only] a Trusted Authority (TA) can reconstruct the true identity of a vehicle from its pseudonym to settle disputes or provide accountability.

2. IDENTITY-BASED CRYPTOGRAPHY

In 1984 Adi Shamir [6] first proposed the idea of an identity-based cryptosystem in which arbitrary strings can act as public keys. However, the first practical identity-based encryption scheme was produced by Boneh and Franklin [1] in 2001. Their scheme uses a non-degenerate, bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are cyclic groups of order p for some large prime p. In particular this map satisfies the following property : $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p$. Weil and Tate pairings on elliptic curves are two fast and efficient ways of constructing such bilinear maps. In addition to encryption, we need the ability to provide non-repudiation in a cost-effective manner. In order to achieve non-repudiation with relatively meager computational requirements, we have chosen to employ identity-based signcryption which combines signing and encryption operations and also produces smaller ciphertext as compared to *sign and then encrypt*. The particular scheme we use was proposed by Chen and Malone-Lee [2]. The costliest computation in this process is the signature verification part with the two Tate pairings. We argue that VANETs are characterized by entities that are not computationally limited and hence have the ability to perform CPU intensive computations like Tate pairings. Overall, the scheme we use, saves one Tate pairing in the decrypt/verify process as compared to other such schemes developed before it.

3. FRAMEWORK DESCRIPTION

In our solution, each vehicle and base-station has a unique identifier ID_{id}. These identifiers include the designation of

*The author acknowledges partial support for this work from Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), Rutgers University, NJ.

VANET'06, September 29, 2006, Los Angeles, California, USA.
ACM 1-59593-540-1/06/0009.

the entity as a vehicle or base-station; e.g. $ID_v = (vehicle \| identifier)$. We envision that these identifiers can be certified at regular periods(say anually) by a TA. If any certificate is revoked the TA notifies all the base-stations in the system, so base-stations have to only store Certificate Revocation List (CRL) entries that are less than a year old. Vehicles never have to download any CRLs, which provides for huge savings in communication costs. We use the following notations:

- d_v, d_I : Secret key corresponding to ID_v and ID_I respectively.
- K_I : Secret key assigned to the base-station I.
- TS_i : Timestamp at time i.
- K^v_{pub}, K^v_{pvt} : Public and private keys assigned to a vehicle by TA as part of their certificates.
- *sigEncrypt* (sigencryption) and *sigDecrypt* (sigdecryption) refer to identity-based operations while *rsaEncrypt*, *rsaDecrypt*, *rsaSign* and $rsaVerify$ refer to operations that use the RSA algorithm. In some places we breakup *sigEncrypt* and *sigDecrypt* to its subfunctions *Sign*, *Encrypt*, *Decrypt* and $Verify$. Additionally, we use *aesEncrypt* and *aesDecrypt* to denote symmetric cipher operations using the AES cipher.

Setup phase: The TA conducts the setup phase [2] of the identity-based cryptosystem and computes the relevant system parameters (*params*) and the master secret s. Both of these are then distributed to all the base-stations in the system. The TA also generates a random secret key K_I for each base-station I and distributes it to that base-station. The TA keeps a copy of this key in its database to help in future arbitration proceedings. The TA provides each vehicle with its unique vehicle identifier (ID_v), public key certificate certifying this identifier and including a public and private key pair (Pub_v and Pvt_v) generated using classical algorithms like RSA. Additionally each vehicle is provided with all the *public* system parameters (params) of the identity-based cryptosystem.

Pseudonym generation : We assume that base-stations have up-to-date CRLs and that they will only issue a new pseudonym only if the vehicle's credentials have not been revoked. When a vehicle needs to get a new pseudonym, it engages a base-station as follows:

$$
\begin{aligned}
ID^i_v \quad &: \quad M = \langle Cert_v, TS_j, ID^i_v, rsaSign_{K^v_{pvt}}(ID_I \| ID^i_v) \rangle \\
ID^i_v \rightarrow ID_I \quad &: \quad C = sigEncrypt_{d^i_v}(ID_I, M) \\
ID_I \quad &: \quad M = \langle Cert_v, TS_j, ID^i_v, U \rangle = sigDecrypt_{d_I}(C) \\
&\quad\; rsaVerify_{K^v_{pub}}(U, ID_I \| ID^i_v) \\
&\quad\; T = aesEncrypt_{K_I}(ID_v \| TS_{j+1})) \\
&\quad\; ID^{i+1}_v = \langle vehicle \| T \| ID_I \| TS_{j+1} \rangle \\
&\quad\; d^{i+1}_v = Extract(ID^{i+1}_v) \\
ID_I \rightarrow ID^i_v \quad &: \quad rsaEncrypt_{K^v_{pub}}(ID^{i+1}_v \| d^{i+1}_v \| TS_j)
\end{aligned}
$$

Secure communication : Our system provides an implicit credential in the form of the pseudonym for secure communication between all entities. The pseudonym includes a time-stamp indicating the last time some infrastructure point validated the credentials of a vehicle. Each vehicle could set its trust threshold as per the user's choice, in deciding how old pseudonyms they want to trust. Once that choice is made, we can simply validate the identity-based signature on the message to verify that the vehicle using the pseudonym actually has the private key corresponding to it. The private key could only have been generated by a base-station (or the TA) who has the master secret s. Due to the contention based nature of medium access control in VANETs, it is important for the security overhead, in terms of the size of the payload and number of additional communication exchanges, be kept low. The implicit authentication provided by our pseudonyms is communication efficient because it eliminates the need for certificate exchange between vehicles and also does not require the vehicles to download any CRLs.

Non-repudiation : In case of a dispute involving vehicles one can try to locate the cause of the incident based on the messages exchanged between vehicles. Vehicles can log messages into some-kind of a black-box like device and turn these messages over to an arbiter. We assume for simplicity that the arbiter is the same as the TA and has access to the secret key database (containing secret keys of the base-stations). Suppose vehicle ID_b hands over a message M and corresponding signature $\langle U, W \rangle$ stating it was sent by vehicle pseudonym ID^i_a to pseudonym ID^i_b. The arbiter will validate if the message indeed was created and signed by ID^i_a, intended for ID^i_b and then will decipher as to which real vehicle ID's these pseudonyms belong to. This mechanism works as follows

1. $M = ID^i_a \| ID^i_b \| m$
2. Check that ID^i_a and ID^i_b are in M
3. If $Verify(M, U, V, ID^i_a) == true$, continue
4. We know $ID^i_a = \langle vehicle \| T \| ID_I \| TS_{j+1} \rangle$
5. $K_I = KeyLookup(ID_I)$
6. $ID = \langle ID_a \| TS_{j+1} \rangle = aesDecrypt_{K_I}(T)$
7. Check that ID contains the same TS_{j+1} as in ID^i_a
8. ID_a is the real identity of the sender.
9. Repeat steps [4..8] with ID^i_b to get recipient.

The advantage of this scheme is that no special storage is required in either the vehicles or the infrastructure for each pseudonym. The message M containing the source and destination pseudonyms and signature are the only things that need to be stored to settle any disputes. Further, the original identities of the vehicles can be re-created only by a TA with valid legal cause for such action.

4. REFERENCES

[1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *Lecture Notes in Computer Science*, 2001.

[2] L. Chen and J. Malone-Lee. Improved identity-based signcryption. *Cryptology ePrint Archive*, 2004.

[3] J. Y. Choi, M. Jakobsson, and S. Wetzel. Balancing auditability and privacy in vehicular networks. In *Q2SWinet*, 2005.

[4] B. Parno and A. Perrig. Challenges in securing vehicular networks. In *HotNets-IV*, 2005.

[5] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In *SASN*, 2005.

[6] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, 1985.