Secure V2V Communication With Certificate Revocations

Ashwin Rao, Ashish Sangwan and Arzad A. Kherani
Indian Institute of Technology Delhi,
New Delhi, India.
ashwin@it.iitd.ac.in,{sangwan,alam}@cse.iitd.ac.in

Anitha Varghese, Bhargav Bellur and Rajeev Shorey
General Motors India Science Lab,
Bangalore, India.
{anitha.varghese,bhargav.bellur,rajeev.shorey}@gm.com

***Abstract*— Secure communication of time critical information in V2V networks is expected to be achieved via a robust infrastructure that provides security related services at all times. This paper explores the dependence of performance of secure V2V communications on the mechanisms used by the security infrastructure. We propose and analyze a performance metric termed the Confidence on Security infrastructure (CoS) that can assist in accepting/dropping a message at each node in V2V communications.**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a kind of an ad hoc network of mobile nodes connected by wireless links. These nodes are free to move randomly and organize themselves arbitrarily. A vehicular ad hoc network (VANET) is a special kind of MANET in which the mobile nodes are vehicles. The main difference between VANETs and MANETs is that in VANETs the nodes move in a random but predictable manner at much higher speeds compared to traditional MANETs.

The advantage of VANETs over traditional ad hoc networks is that the nodes (vehicles) possess substantial power resources. VANETs enable vehicles to communicate with each other (V2V) and the roadside infrastructure (V2I) to increase the awareness about their surroundings, thereby increasing safety and possibly optimizing traffic. The applications running over VANETs are be broadly classified as

- Safety related applications - e.g., Emergency Messages
- Best effort applications - e.g., Infotainment
- Secure Transactions - e.g., Toll collection

Most of the critical messages in VANETs are broadcast oriented safety messages that need to have a deep penetration and be delivered in a short time. Additionally these messages must be secure and must not leak personal, identifying, or linkable information to unauthorized parties, as the owners of the vehicles involved in the communication have right to privacy. Thus the important points in VANET security are

- Authentication - There can be malicious and genuine sources for messages in VANETs. Authentication is the ability to distinguish between these sources.
- Anonymity - The physical identity of the originator of a message should not be extractable from the message.
- Data Integrity - The data received is exactly as sent by the authorized entity without any modification [1].
- Low Overhead - The messages being time critical, the security overheads should retain the usefulness of the message.

The IEEE 1609 family of standards, provides a set of the specifications for the Wireless Access in Vehicular Environments (WAVE) communication protocols to be used in VANETs. A part of this family is the IEEE P1609.2 [2] that defines the secure message formats and techniques for processing these secure messages within the DSRC [3] system using the Public Key Infrastructure(PKI). It also covers methods for securing WAVE management and application messages and describes administrative functions necessary to support core security functions, such as revoking the certificate issued to a vehicle.

II. OVERVIEW OF PKI: A VANETS PERSPECTIVE

The public key infrastructure is based on asymmetric key cryptography. Each principal in a Public Key Infrastructure (PKI) system has a pair of keys: (Private key, Public key). The *private key* is known only to the principal, whereas the *public key* can be shared with all the entities in the system. The keys can be visualized as a pair of functions $P_r(.)$ and $P_u(.)$ representing the private and public keys respectively, having the property

$$M = P_r(P_u(M))$$

$$M = P_u(P_r(M))$$

where M is the message that is to be secured using the keys.

To ensure message integrity, the source of the message *signs* the (hash of the) message with its private key, and appends this *signature* along with the message. Upon receiving this message, the recipient can verify the signature of the message using the (sender's) *public key*. A fundamental problem in this approach is the exchange of the keys without compromising them. One widely accepted solution is for trusted nodes [4] known as Certificate Authorities (CA) [5] to digitally sign data structures known as *certificates*, that state the binding between the owner of the private keys to its corresponding public keys.

978-1-4244-1690-5/07/$25.00 ©2007 IEEE.

In the case of the IEEE 1609.2 Standard, an (unsigned) certificate has several fields including

1) The public key
2) The expiry time of the certificate
3) The Certificate Revocation List (CRL) series corresponding to the certificate.

The certificate issued by the CA contains the above fields and the signature of the CA. Note that the *Public Key of the CA*, assuming only one CA for the whole system, must be available at each entity of the PKI system in order to verify the certificates signed by the CA. As distribution of all the certificates issued by a CA is impractical, IEEE 1609.2 Standard specifies that a signed message includes the certificate of the sender containing the public key used to sign the message.

Certificates that were signed by a CA can also be revoked due to various reasons, that are beyond the scope of this document. A proposal for certificate revocation in vehicular networks includes temporary revocation of the attacker until the connection with the CA is established [6]. Once a certificate is revoked, the revocation information is propagated using certificate revocation lists (CRLs) that contains (but not limited to) the following fields

1) CRL series number: The CRL series this CRL is for
2) Entries: List of all the revoked certificates

Thus the cost of verifying the message also includes the cost of confirming the presence/absence of certificates in the CRLs available at the time of verification of the message. Hence, for the robustness of the operation, timely access to this revocation information is important. Real time availability of CRLs is a particularly hard problem in vehicular networks.

III. Need for a Robust Algorithm to Accept/Drop Messages

VANETs may consist of some *compromised* nodes (vehicles or static nodes). It is precisely to counter such nodes, IEEE 1609.2 allows for the possibility of revocation of certificate of a vehicle, while leaving out the mechanism used to identify a compromised vehicle. Further, IEEE 1609.2 proposes use of PKI to propagate the revocation information through the VANET in the form of Certificate Revocation Lists (CRLs).

Due to storage space constraints at an OBU or because of infrequent OBU-PKI interactions, the CRL available at an OBU may not be complete or accurate. Since a message received by an OBU could have originated from a compromised vehicle, in order to improve the (reliability) performance of the message flow in V2V communications, the receiving OBU needs to know when to accept/drop a message at the security layer.

Clearly, if a receiving OBU finds the sender of the message in one of its stored CRLs, it will drop the message, knowing for sure that the sender is a compromised entity. However, absence of the sender in the CRLs available at the receiver does not guarantee that the sender's certificate has not been revoked.

We propose that any algorithm for accepting/dropping a message be evaluated based on the performance metric that we call the *Confidence on the Security infrastructure (CoS)*. The CoS is defined to be *the probability that the sender's certificate has not been revoked if it is not in the CRL available at the receiving OBU*. The CoS is dependent on

- How recent the current certificate is, i.e., the freshness of the certificate [7]. This freshness complements the honest majority concept of vehicular networks that assumes most of the nodes in the V2V are honest, but the cost of obtaining this freshness needs analysis for various security infrastructure models [4].
- The freshness of the CRLs present in the OBU: Freshness of CRLs answers the question "How recent are the CRLs present in the OBU compared to those issued by the PKI?" The freshness of CRLs in the OBU is the penetration capacity of the CRLs, which in turn is completely dependent on the mechanism used for issuing certificates and distribution of the CRLs.

Associated with any algorithm for accepting a message is the probability that a message from a non-compromised sender is dropped. The relation between CoS and this probability of *false drop* depends on at least all those factors on which CoS itself depends. Though finding such a relation will be an interesting study, we restrict ourselves to study of CoS alone in this paper. We now propose an algorithm to accept a message whose sender does not appear on the CRL of the receiving OBU and then present a first order analysis that incorporates key design parameters.

IV. Analytical Approach: Finding the CoS for VANET

We assume presence, at some fixed points over region of interest, of info-fueling stations[1] that are visited rather infrequently by the vehicles (inter-visit time is random, with an average of order of days). These info-fueling stations provide the visiting vehicles with the up-to-date CRLs.

We now provide an example analysis on how to compute CoS of the system, i.e., the various system parameters that affect the CoS.

We consider a system with very large number of vehicles moving according to some mobility model, and each vehicle owns a certificate for signing the messages. Consider a tagged vehicle and define the counting process $\{c(t)\}_{t\geq 0}$ that counts the number of other vehicles that have sent messages to the tagged vehicle by time t. Thus the rate at which the tagged vehicle comes in contact of other vehicles using V2V communication is

$$\lambda = \lim_{t\to\infty} \frac{c(t)}{t},$$

assuming the limit exists almost surely. Clearly $\{c(t)\}_{t\geq 0}$ is a random process.

[1] Gas stations that provide fuel to the vehicle and connectivity with the PKI to the OBU

978-1-4244-1690-5/07/$25.00 ©2007 IEEE.

Now consider another random process $\{r(t)\}_{t\geq 0}$ that counts the number of certificates revoked by time t, and define the long term revocation rate as

$$r = \lim_{t\to\infty} \frac{r(t)}{t}.$$

Since we are interested only in the average behavior of a large population of vehicles, we will assume that the process $\{c(t)\}$ is not significantly affected by (or, coupled to) the process $\{r(t)\}$. However, such a coupling between $\{c(t)\}$ and $\{r(t)\}$ needs to be accounted for when considering a finite population of vehicles.

The tagged vehicle refreshes its CRLs by communicating with the CA (via RSUs or info-fueling stations) according to some independent point process, $\{m(t)\}_{t\geq 0}$, where $m(t)$ is the number of such CRL updates by the tagged vehicle by time t. We will assume that the inter-update times (the time between successive CRL updates) come from a sequence of independent and identically distributed random variables $\{T_i\}_{i\geq 1}$. Let $E[T] := E[T_i]$ and $E[T^2] := E[T_i^2]$. Since we are interested in time average behavior of system (the CoS), we assume that the tagged vehicle updates its CRL at time 0.

We will assume that the inter-transition times of all the three counting processes under study have finite second moment. Further, we will assume that the processes $\{c(t)\}$ and $\{r(t)\}$ vary at a faster time scale compared to that of the $\{m(t)\}$ process, i.e., $\frac{1}{\lambda} << E[T]$ and $\frac{1}{r} << E[T]$. This assumption, along with the finiteness of the second moments of inter-transition instants, imply that $m(t)$ process sees an averaged-out version of the other two processes.

This conclusion, though not entirely correct, provides us with a good first order approximation of the system that enables us to perform a tractable and meaningful analysis.

Just after time $t = 0$, the tagged vehicle is able to accept/drop messages with full confidence because its CRL is fresh. However, as time passes, the number population of vehicles with revoked certificate, the tagged vehicle is unaware of, increases linearly with time (with a slope r) and their chances of meeting the tagged vehicle also increases linearly with time (with a slope $r\lambda$). Thus, by time t the tagged vehicle would have met

$$d(t) = \int_{u=0}^{t} r\lambda u du = \frac{r\lambda t^2}{2} \tag{1}$$

vehicles with revoked certificate. Since these vehicles do not appear on the CRLs available with the tagged vehicle, it will accept all messages from such vehicles. Thus by time T_1, at which the tagged vehicle updates it CRL, it would have accepted $d(T_1)$ such communications (that were not to be accepted).

This process renews itself at time instants $\{T_i\}$ so that the number of messages from compromised vehicles accepted by the tagged vehicle would be given by the random process $\{D(t)\}$ defined as

$$D(t) = \sum_{i=1}^{m(t)} d(T_i) + d(t - \sum_{i=1}^{m(t)} T_i).$$

By definition, the rate of accepting messages from compromised nodes q is

$$q = \lim_{t\to\infty} \frac{D(t)}{t} = \frac{E[d(T_1)]}{E[T_1]},$$

where the equality follows from Elementary Reward Theorem [8].

For a given λ, the rate at which the tagged vehicle comes in contact of other vehicles using V2V communication, the probability of accepting the messages signed by revoked certificates, i.e., from the nodes whose certificates are revoked at the PKI but their corresponding CRL entries in the CRL lists at the OBU are absent, is given as $\frac{q}{\lambda}$.
Hence by definition

$$CoS = 1 - \frac{q}{\lambda} = 1 - \frac{rE[T^2]}{E[T]}$$

$$\therefore CoS = 1 - \frac{rVar(T)}{E[T]} - rE[T] \tag{2}$$

The following conclusions can be made from the above equation.

- The CoS is independent of λ, the rate at which the tagged vehicle comes in contact with other vehicles using V2V communication.
- The CoS decreases as the rate of revocation r increases; this is in accordance with intuition.
- The CoS decreases as the expected time $E[T]$ of CRL updates increases
- An increase in variance of the inter-update times for CRL actually decreases the CoS even for the simple system/algorithm under consideration.

An important observation from the expression for CoS is its dependence on the quantities $E[T^2]$ and $E[T]$. *This linear form of dependence of CoS on $E[T^2]$ is not entirely obvious at an intuitive level*, the analysis thus provides significant insight into the system's working and performance. Hence updates of CRL lists at regular intervals maximizes the CoS for a given rate of revocation r.

Clearly, one way to increase CoS is to reduce the variance of the CRL update times and, for small variance $Var(T)$, one needs small value of $E[T]$ to obtain large CoS. Since the times between CRL updates are completely determined by the mobility pattern of vehicles and location of RSUs, it is bound to be a random variable. RSUs being sparse in the network imply significant variance for most of the mobility models.

In order to make the system behave like the one where the CRL update intervals are deterministic and small (such that the variance is 0 and CoS is large), we propose the following scheme:

- **Freshness check**: Each node performs a freshness check on its certificate, that is successful if the certificate is not

978-1-4244-1690-5/07/$25.00 ©2007 IEEE.

revoked. The details of the freshness check are provided in section V.

- **Accept/Drop mechanism**: Any vehicle maintains a window of T_r time units. For any received message, a receiving OBU drops the message if
  a) either the sender happens to be in its CRL or,
  b) the sender has not done a freshness check in the last T_r time units. The message is accepted otherwise. We will refer to the window T_r as the *freshness threshold.*

This simple scheme, as already mentioned, is aimed at achieving a CoS that one would have obtained under zero variance ($Var(T)$) and small update times ($E[T] = T_r$). As will be seen later, *the time window T_r will now act as effective CRL update times* so that the variance is considerably reduced and the mean (required $E[T]$) is under OBUs control. (Note that the inter CRL update times are governed by the user mobility pattern that can not be controlled by the OBU.)

The equation for CoS using the concept of freshness now becomes

$$CoS = 1 - rT_r \qquad (3)$$

$T_r > \frac{1}{r}$ results in negative values of CoS, hence the threshold for freshness checks should be less than the average revocation time to have a $CoS > 0$. For a given rate of revocation the CoS increases as T_r decreases, so it is desirable to have T_r as small as possible. Clearly, the time window T_r can not be too small as it will

1) result in almost all messages being discarded, and
2) require the OBUs to do freshness check very frequently if it does not want its message discarded by the receiving OBU. However, there is a natural upper bound on the rate at which an OBU can undergo freshness check because of the maximum rate at which it crosses RSUs; this bound clearly depends on the mobility pattern of the vehicles and the placement of RSUs.

Note that the time window T_r used by vehicles determines the required rate of freshness checks by other OBUs. We propose that the PKI computes, depending on the state of the system (that includes the computation load on the PKI), the time window T_r and the average freshness check interval, say T_c ($T_c < T_r$), used by *all* the OBUs in the network.

V. Freshness of Certificates

The freshness of the certificate complements the honest majority principle and is based on the following assumptions

- The sender and the receiver of a signed message have an equal access to the PKI, which in the case of VANETs is available at irregular intervals.
- The system should minimize the time for which malicious nodes can operate.
- For the safety of the passengers, each OBU requires the safety messages generated by it to have a deep penetration in VANETs.
- The verifying time of signed messages needs to be minimized.

Each vehicle generating signed messages owns certificates signed by the CA that are valid for a finite amount of time, but a certificate can be revoked during the validity period without the knowledge of the OBU. Assuming that the RSUs along with other info-fuelling stations provide connection to the PKI, the OBU can query to check if one of its certificates (that is still valid) is revoked.

We propose adding a new field C_f in the certificate that indicates the last time a successful freshness check was carried out. The number of bits for this field shall depends on the granularity of the freshness check threshold T_r. This field initially has *the time of issue* of the certificate and is updated during subsequent freshness checks. During a freshness check the OBU sends a signed message to the PKI containing the freshness check request. If the certificate is not revoked, the CA sets the C_f field as the current time and signs the certificate. If the certificate is revoked then this field is set to 0, to indicate the failure of freshness check. The receiver of signed messages can now accept or drop messages based on the freshness of the certificates. The steps involved in the freshness check at the PKI are as follows

1) Verify the signature of the freshness check request message sent by the OBU using the *public key* that is part of the message itself
2) If the certificate is not revoked then set the freshness check time in the certificate to the current time else the freshness check time to 0, indicating that the certificate is revoked.
3) Sign the certificate with the private key of the CA

This is fundamentally different from issuing new certificates and the concept of short-lived certificates as

- New keys are not being generated, hence the cost of generating key pairs is avoided.
- The other fields of the certificate are not modified (or generated by the CA).
- The expiry time of certificate remains the same as new keys are not generated, hence the effective time for which the certificate can be used is from the time of freshness check to the expiry time.

The disadvantages of above scheme can be listed as follows

- If the certificate of the CA is compromised then freshness checks shall not work and the number of packets accepted from compromised nodes shall follow equation 1.
- For all practical reasons the freshness check threshold (T_r) cannot be less than the average freshness check interval (T_c). Hence, for a given value of T_c that is dependent on the mobility model and the number of RSUs present in a geographical region, the CoS decreases as the rate of revocation increase.

978-1-4244-1690-5/07/$25.00 ©2007 IEEE.

The advantages of having a freshness field in the certificates can be listed as follows

- As the receiving OBU accepts or drops messages based on the freshness of the certificate, the time of verifying the message is *constant* and is *independent of the number of revoked certificates present in the CRLs.*
- The OBU need not store the CRLs for vehicles. This *reduces the storage space* required in OBUs and can nullify the problem of distribution of CRLs.
- Without freshness, the time for which a compromised node can cause chaos is the average CRL update time, but with freshness the operating time is now limited to T_r (the freshness check threshold).
- On revocation of a certificate, if the freshness check of certificate fails then the OBU can stop using the certificate thus *reducing the number of messages signed by revoked certificates.*
- In case of short-lived certificates the validity period is limited to the average time interval between consecutive PKI interactions. Here the certificate can be valid for longer duration and based on the revocation rate (r) and the required CoS, the OBU receiving signed messages *can decide the* T_r (or PKI can advertise this value) obtained from equation 3, to accept and drop the message.

VI. Numerical Results

We incorporated the freshness check mechanism in the *ns2* network simulator. 200 vehicles are moving around in a square region of side 2400 meters according to the mobility model proposed in [9]. There are 4 static RSUs spread across the region of mobility that provide connectivity with the PKI.

Each vehicle does a freshness check whenever it is in contact with any of the RSUs. The receiver keeps a *freshness threshold* so that it accepts messages only from those vehicles that have performed a freshness check within this time window that was varied from 200 secs to 350 secs. By the end of the simulation 40 vehicles have their certificate revoked.

We study a tagged vehicle that has done a CRL update at time 0 (assuming that it never does a CRL update again). Each of the 200 nodes having a transmission range of 200 meters periodically transmit packets once every 300 ms. The freshness check threshold (T_r) is 250 seconds in a simulation that lasted 5000 seconds. The number of packets accepted from compromised nodes with and without freshness during the first 3000 seconds of the simulation is show in Figure 1.

The vertical lines in Figure 1 show the times at which the revocations took place. Without freshness checks, according to equation 1, by time t the tagged vehicle would have met $d(t)$ vehicles with revoked certificate. This value of $d(t)$ according to equation 1 is directly proportional to

- The revocation rate r
- The rate of communication with other nodes λ.
- The square of the time t

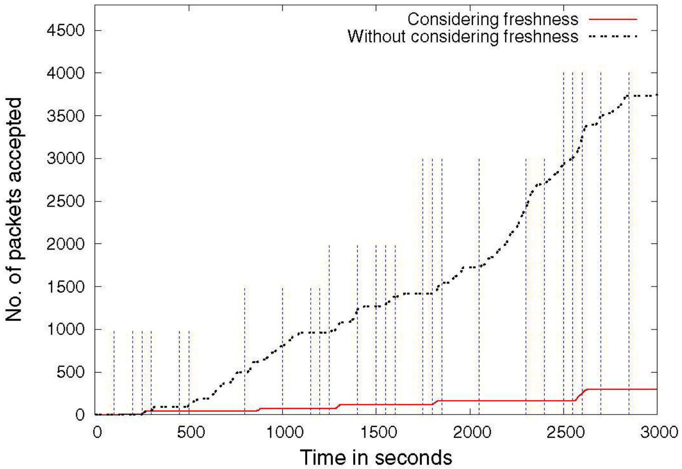

Fig. 1. Packets from compromised nodes

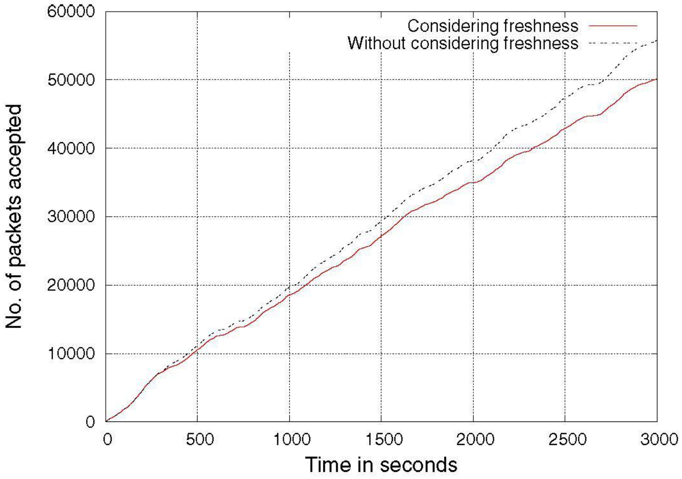

Fig. 2. Packets from non-compromised nodes

Hence, the number of packets accepted from compromised nodes increases exponentially as time increases. But when the freshness is introduced, this exponential increase is seen for a maximum of T_r seconds only if the node is revoked within the T_r seconds after the freshness check. Without freshness checks the window of operation of the compromised nodes would be the average CRL update interval but in this case it is clearly seen to be limited by T_r. But freshness checks comes at a cost. The number of packets from non-compromised nodes is also reduced. This is shown in Figure 2

Figure 3 gives the evolution of fraction of packets *actually accepted* from compromised vehicles (whose certificate has been revoked) for various values of T_r. The plot also gives the fraction of packets *accepted* from vehicles whose certificates are not revoked. An important observation from this plot is that using freshness check we are able to filter out most of the messages from compromised vehicles, *while at the same time maintaining a significant acceptance rate from non-compromised vehicles.* The plot also brings out the dependence of performance of our scheme on the parameter T_r; this is the reason we propose that the PKI compute an *optimal* value of T_r and advertise it to the OBUs for their use.

978-1-4244-1690-5/07/$25.00 ©2007 IEEE.

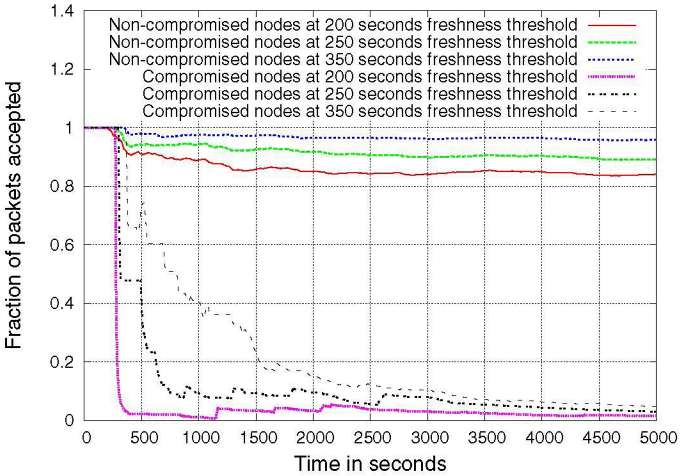

Fig. 3. Fraction of packets accepted from a) compromised vehicles, and b) non-compromised vehicles.

VII. Scope for Extension

Freshness checks need to be done periodically for maintaining the required value of CoS. The overheads of doing freshness checks in terms of computation at the PKI along with the impact of the freshness check messages on the performance of V2V communication needs to be studied.

The algorithm to accept and drop messages based on freshness checks results in packets from non-compromised nodes to be dropped, hence the relation between the CoS and the probability of a message from a non-compromised node getting dropped at the OBU needs to be analyzed.

VIII. Conclusion

Certificate revocation is required in VANETs to prevent malicious nodes from creating havoc, and the process of revocation is complete only if timely access to this revocation information is made available. This paper tries to address the problem of access to revocation information using a concept called freshness, that does not require the PKI to distribute the CRLs and the OBUs to maintain the CRLs. This reduces the storage requirement at the OBU and provides a constant time algorithm, that is independent of the number of certificates revoked, to verify the a signed message.

References

[1] W. Stallings., *Cryptography and Network Security*. Pearson Education International, 2006.

[2] *Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, IEEE Std. 1609.2, 2006.

[3] "Standard specification for telecommunications and information exchange between roadside and vehicle systems - 5GHz band dedicated short range communications DSRC medium access control MAC and physical layer PHY specifications," ASTM, 2006.

[4] R. Perlman, "An overview of PKI trust models," *IEEE Network*, pp. 38–43, 1999.

[5] R. Housley, W. Ford, W. Polk, and D. Solo., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC 3280, 2002.

[6] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J. P. Hubaux, "Certificate revocation in vehicular networks," LCA Report, Tech. Rep. 2006-006, 2006.

[7] R. Rivest, "Can We Eliminate Certificate Revocations Lists?" in *Financial Cryptography*, 1998, pp. 178–183.

[8] R. Wolff, *Stochastic Modeling and the Theory of Queues*. Prentice Hall, 1989.

[9] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad-hoc networks." in *Vehicular Ad Hoc Networks*, 2004, pp. 91–92.