Probabilistic Key Distribution in Vehicular Networks with Infrastructure Support

João Almeida*, Saurabh Shintre*†, Mate Boban*†, and João Barros*

* Instituto de Telecomunicações, Departamento de Engenharia Electrotécnica e de Computadores,
Faculdade de Engenharia da Universidade do Porto

† Department of Electrical and Computer Engineering, Carnegie Mellon University

Email: {jpa, saurabh.shintre}@fe.up.pt, mboban@cmu.edu, jbarros@fe.up.pt

***Abstract*—We propose a probabilistic key distribution protocol for vehicular network that alleviates the burden of traditional public-key infrastructures. Roadside units act as trusted nodes and are used for secret-sharing among vehicles in their vicinity. Secure communication is immediately possible between these vehicles with high probability. Our performance evaluation, which uses both analysis and simulation, shows that high reliability and short dissemination time can be achieved with low complexity.**

I. Introduction

Vehicular Ad-hoc Networks (VANETs) are expected to enable increased safety, enhanced driving experience, and improved traffic efficiency. These networks are characterized by short-lived pairwise connections, which makes the network topology highly dynamic. Furthermore, single trip of a vehicle may involve communication with a large number of other vehicles. Dependence on such technology, however, may turn hazardous if not implemented securely, particularly due to the vulnerability of the wireless medium to passive and active attacks.

Messages exchanged in a VANET have different roles, thus requiring different security measures. For instance, securing safety messages requires the deployment of a scheme that would privilege authentication over confidentiality [1], since the information contained in the message is not particularly sensitive and may be of interest to multiple users, while the legitimacy of the source is important. These applications lie at the heart of vehicular networks, and perhaps for that reason it is generally considered that integrity and authentication are of greater concern than confidentiality. Therefore, most security schemes adopt vehicular public key infrastructures (PKI), e.g., [2], [3] that, in general, make use of public key cryptography (PKC) for authentication. A large number of applications and services that could be deployed in VANETs may depend on confidential data transmission. These applications range from driver assistance systems (e.g., [4]) to traffic information systems (e.g., [5]) and infotainment applications (e.g., [6]). Although PKC could also be used for encryption, efficiency dictates that the best course of action to provide confidential transmission is to use symmetric encryption with a shared secret [7]. However, PKC solutions are not adequate for noisy environments since they generally employ several rounds of interaction between users. Furthermore, in dense networks, the overhead of message transmission and signature verification can be prohibitive [1].

We provide an alternative solution to the problem of key management in vehicular networks using the concept of randomized key pre-distribution (RKPD) [8]. Since in RKPD keys are computed from the common information possessed by vehicles, interaction between users for key agreement is minimized. The proposed protocol does not intend to replace PKI-based schemes, since it is not aimed at guaranteeing authentication. Rather, it is envisioned to be a lightweight key distribution service that transparently enables network nodes to form a shared secret, allowing them to establish secure connections via symmetric encryption with implicit key agreement.

Our main contributions are as follows:

- *Key distribution protocol:* We propose a probabilistic key distribution protocol that enables vehicles to establish secure pairwise connections with arbitrarily high probability of success and low communication complexity. The protocol exploits spatially bounded communication patterns that are present in VANETs by advertising the common keys between vehicles that are near each other.
- *Security and performance analysis:* We analyze the effectiveness of establishing a secure connection, as well as its robustness with respect to eavesdropping attacks. Our simulations highlight the efficiency of the protocol, as well as the trade-offs between the density of trusted nodes and the speed of information dissemination.

The rest of the paper is organized as follows. Section II provides a discussion on the existing solutions to the problem of secret key sharing in vehicular networks and motivates a distributed and probabilistic key-sharing approach. The system setup and proposed protocol are presented in Section III. Section IV analyses the security of the scheme. In Section V

This work was partly supported by the Portuguese Foundation for Science and Technology (under the Carnegie-Mellon|Portugal program through the DRIVE-IN project CMU-PT/NGN/0052/2008 and grants SFRH/BD/33771/2009 and SFRH/BD/71350/2010, the MIT|Portugal Program through the MISC project MIT-PT/TS-ITS/0059/2008 and under the grant SFRH/BD/60831/2009) and the European Commission under grant FP7-Capacities-RegPot-316296 (Future Cities - Expand the Centre of Competence in Future Cities of the University of Porto to Strengthen Inter- Disciplinary Research and Knowledge Transfer to the Industry in the Norte Region of Portugal).

we discuss the model and environments under which the protocol is analyzed. Section VI discusses several operational aspects of the proposed scheme and Section VII concludes the paper.

II. Related Work

Due to the vital role of authentication, proposed VANET security frameworks rely heavily on PKC. Consequently, most of the research focuses on the design of PKI-based key management systems for pairwise or group communication (e.g., [1], [9]). When symmetric encryption is required, it is expected that nodes perform some well-known key agreement schemes or use integrated encryption schemes. In particular, the IEEE 1609.2 standard specifies the Elliptic Curve Integrated Encryption Scheme as the asymmetric encryption algorithm [3], which is based on Diffie-Hellman key agreement. In [9], an architecture was proposed for secure vehicular communications, which includes a key management scheme. Certification authorities (CAs) are responsible for managing the identity and credentials of vehicles registered within a given region. Each node is registered only in a given CA, which provides it with a unique ID, a long-term pair of private/public keys and a long term certificate. To achieve secure communication, short-term private-public key pairs and certificates are used. These are internally generated by the node and signed by the CA. Raya and Hubaux [1] designed a security framework for VANETs based on PKI. A protocol is proposed which uses the geographic location of vehicles. In the protocol, a geographic group is formed, which elects a group leader, responsible for distributing a group key to its members, enabling secure communication within the group. In any scenario where the protocol cannot function properly, the fall-back to a simple digital signature scheme is ensured.

In practice, VANETs are characterized by a dynamic topology and link disconnections are frequent. Moreover, sporadic and burst errors are common due to the presence of signal propagation obstacles that lead to shadowing [10]. Therefore, it is crucial that the key agreement protocol makes use of the least possible interaction between users in order to minimize the overall delay in the key establishment procedure as well as maximizing the probability of success. This can be achieved by means of probabilistic key distribution schemes. However, due to the size and dynamic nature of these networks, key pre-distribution is unfeasible. To circumvent this problem, we use the infrastructure supporting the vehicular network, which will be responsible for assigning and efficiently distributing keys.

III. Key Distribution Scheme for VANETs

A. Network Model

We assume a VANET is composed of nodes which can be mobile (vehicles) or static (road-side units or RSUs). Further, we assume that a VPKI is in place, so that nodes possess at least one pair of public-private keys and the corresponding certificates, issued by CAs. Each CA is responsible for a specific geographic region (e.g. one or more highways, an urban area, etc.) and acts as the root of trust for a VANET. The RSUs are infrastructure-based devices located next to the road, and therefore provide coverage within a given radio range. Ideally, the deployment coverage should be such that any vehicle can contact an RSU when entering a specific region controlled by a CA. However, it is important to note that the protocol can function even in environments with sparsely deployed RSUs. Additionally, we consider that RSUs have a permanent connection to some CA. Vehicles are equipped with on-board units (OBUs) and IEEE 802.11p radios. We do not make assumptions on the penetration rate of equipped vehicles. Key dissemination is enabled by RSUs, albeit a more general case can be considered where key dissemination is enabled by any trusted node (static or mobile).

B. Key Distribution Protocol

The goal of the proposed scheme is to enable any two vehicles to establish a secure connection via a shared key. Each vehicle entering a certain geographic region requests a set of keys from an RSU that is within that region. We allow users to contact RSUs in one of two ways: a) through *direct communication* (i.e. when an RSU is within communication range) or b) through *multi-hop communication* (in which case vehicles flood a key request message to the network). The former approach limits the number of messages flooded in the network. On the other hand, it requires higher RSU density for a timely bootstrap, i.e., to satisfy the key requests immediately. The latter is more robust to sparse RSU densities, while being more prone to active attacks by intermediate nodes.

More precisely, let vehicle V send a key request message to an RSU with its public key K_V. The RSU draws a ring of k keys out of a pool of N keys, and sends the node the set of keys $\mathcal{K}_V$ (encrypted with the node's public key), along with the respective identifiers. Additionally, the RSU sends to node V a list of identifiers of the common keys shared by V and the set $\mathcal{N}(t)$ of vehicles that have contacted the RSU at most t seconds ago. By exploiting this information about nearby vehicles, vehicle V will be able to immediately establish a secure connection with the vehicles in $\mathcal{N}(t)$ without further interaction, as long as they share some keys. The RSU also informs its x-hop neighborhood, $\mathcal{N}_x$, about the presence of vehicle V, broadcasting the identifiers of its keys. This allows the vehicles in $\mathcal{N}_x$ to have fresh information about incoming vehicles that are geographically close. Suppose that two nodes share s keys, $k_1, \ldots, k_s$, with $s > 0$. They secure the communication link by deriving a new shared secret $K = f(k_1, \ldots, k_s)$, where $f(\cdot)$ is a cryptographic hash function.

Fig. 1 illustrates the key dissemination procedure. Here, node A requests a set of keys to RSU R$_3$. Suppose this RSU has been contacted by all the nodes in the figure in the last t seconds, i.e. $\mathcal{N}(t) = \{B, C, D, E, F, G\}$. R$_3$ will send A a list of all the key identifiers these nodes have in common with it. Now consider that R$_3$ will inform its 1-hop neighborhood, $\mathcal{N}_1 = \{B, C, D, F\}$, about the keys assigned to A. Assuming that A shares keys with these nodes, it can communicate securely with the set $\{B, C, D, E, F, G\}$, while at the same time the set $\{B, C, D, F\}$ can also communicate securely with A.

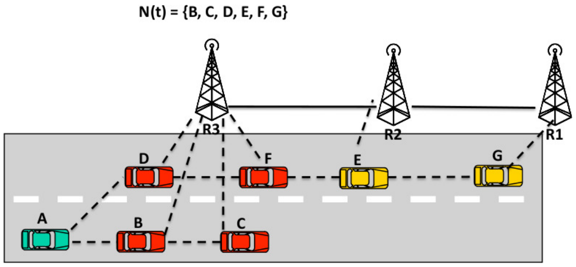

Fig. 1. Example of the key request procedure.

The information flowing in the network is asymmetric and nodes might not be aware of other nodes' keys. With respect to the asymmetry, there are two cases that need to be taken into account. If the sender is not aware of the receiver's keys (that information has not reached him yet), both nodes need to broadcast key identifiers to find the common keys and proceed as before to compute the shared secret. The other case is when they do not have shared keys. In this case, they can fall-back to one of the standard key agreement approaches.

It should be stressed that exposing identifiers of the keys does not directly compromise secure communication, since an attacker has to possess all the keys used to secure the link [8]. If an attacker compromises other vehicles, the keys he obtains are still random keys, thus knowing a priori the shared keys does not increase its probability of compromising a link.

IV. Security Analysis

A. Threat Model

In this work we consider applications with confidentiality requirements, and therefore assume solutions are in place to solve other possible security issues. Confidentiality implies keeping the contents of messages secret to all users, except the authorized ones. In this context we assume passive attackers, and we mainly focus on mitigating eavesdropping attacks. Although passive attacks impose less risks to the safety of the vehicular network users, in general, they are also more difficult to detect than active attacks.

We assume that the messages exchanged over the wireless links are encrypted. Under the assumption that the eavesdropper is unable to break the underlying cipher, his goal is to gain access to the key that is used to secure the link. Note that the presence of an eavesdropper is generally oblivious to both legitimate users. Moreover, users that comply with the communication protocol and are part of the network may also eavesdrop on other users.

B. Probability of Secure Connection

As mentioned in Section III, the key used to encrypt the communication link is a function of intersection of the key sets assigned to each user. This means that adversaries can successfully attack a link if they possess all the keys used to compute the shared secret. In this context, a group of colluding eavesdroppers can be seen as a single eavesdropper with access to a larger set of keys.

Let $\mathcal{K}_A$ and $\mathcal{K}_B$ denote the ring of keys possessed by nodes A and B, respectively. Additionally, let $|\mathcal{K}_A| = |\mathcal{K}_B| = k$, and let the pool size be N. Let an eavesdropper contain a set of keys $\mathcal{E}$, with $0 \le |\mathcal{E}| = k' \le N$. As the presence of this eavesdropper is not known, we do not know which keys are compromised. Nevertheless, we can estimate the amount of keys required to compromise the security of pairwise connections. Let $P(|\mathcal{K}_A \cap \mathcal{K}_B| = s)$ denote the probability that two legitimate nodes share exactly s keys, $0 \le s \le k$. We have that

$$P(|\mathcal{K}_A \cap \mathcal{K}_B| = s) = \frac{\binom{N}{s}\binom{N-s}{k-s}\binom{N-k}{k-s}}{\binom{N}{k}\binom{N}{k}}.$$

Let the number of neighboring nodes at a given time be d. A link is secure with respect to its neighboring nodes if nodes share at least s keys, with $s > 0$, and these s keys are not compromised by d neighbors. The probability that a link is secure is given by

$$P_S = 1 - \sum_{s=0}^{k} P(|\mathcal{K}_A \cap \mathcal{K}_B| = s)\left(1 - \left(1 - \frac{k}{N}\right)^d\right)^s.$$

Let us define outage as the event that an eavesdropper with access to a set of keys $\mathcal{E}$ is able to compromise the security of a link. The outage probability can then be defined as

$$\begin{aligned} P_{outage} &= P(\mathcal{K}_A \cap \mathcal{K}_B \subseteq \mathcal{E}) \\ &= \sum_{s=0}^{k} \frac{\binom{N}{s}\binom{N-s}{k-s}\binom{N-k}{k-s}\binom{N-s}{k'-s}}{\binom{N}{k}^2\binom{N}{k'}}. \end{aligned}$$

We are interested in the trade-off between P_S and P_{outage}. On one hand, we require that the probability of establishing a secure connection be arbitrarily high, i.e., users are able to derive secret keys even in the presence of a possibly large amount of neighbors. On the other hand, we are also interested in keeping the outage probability vanishingly small for the chosen parameters, such that colluding eavesdroppers are not able to compromise the system. Figure 2 shows the probability that a secure connection can be established in presence of d neighbors, each one having k keys. As the number of neighbors increases, the probability of having a secure connection diminishes. However, the scheme shows some robustness for a reasonable numbers of neighbors: for a pool of $P = 100000$ keys, distributing $k = 1500$ keys is sufficient to have an almost certain secure connection up the presence of 100 neighbors. On the other hand, Fig. 3 shows the outage probability as a function of the number of keys k' obtained by colluding eavesdroppers and the number of keys k given to each user. In particular, for a pool of $P = 100000$ keys, if $k = 1500$ keys are distributed to each vehicle, an eavesdropper who collects approximately $k' = 40000$ keys

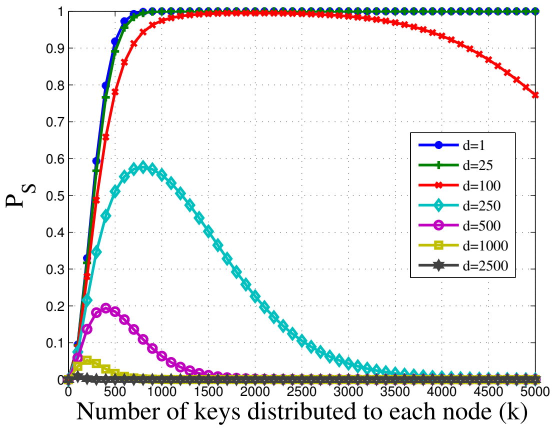

Fig. 2. Probability of two nodes sharing a secret key not possessed by any of their d neighbors. Key pool size $P = 100000$.

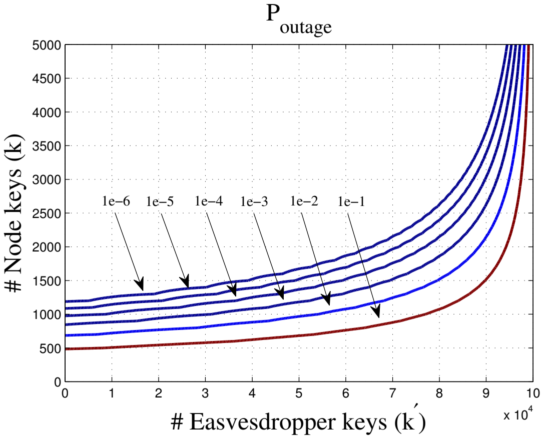

Fig. 3. Outage probability for $P = 100000$. Lines are for a probability of outage of respectively $P_{outage} = [1e-1, 1e-2, \ldots, 1e-6]$.

only has a probability $P_{outage} = 10^{-6}$ of compromising a link, thus showing the system is fairly robust.

C. Reliability

Analyzing the reliability of a key distribution scheme in a dynamic scenario such as a vehicular network is a complex task.We compare our scheme with a basic version of the Diffie-Hellman (DH) key agreement [7] assuming an end-to-end erasure model, where packets are lost with probability ϵ.

Assume that node A wishes to share a secret with node B. In the DH protocol, each nodes transmits a message prior to computing a shared secret. Additionally, the two nodes must acknowledge the reception of both packets, which gives four transmission in total. In our protocol, if A and B share keys assigned by the RSU and are aware of the common keys, they already possess a shared secret. If they are unaware of the common keys, they will broadcast their key identifiers and acknowledge the reception of this information, i.e., they will use the same number of transmissions as a DH scheme. Lastly, if they do not share keys, they will fall-back to the DH scheme.

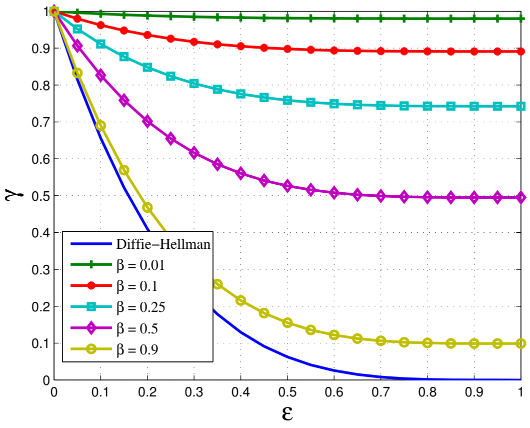

Fig. 4. Probability that two nodes are able to share a secret without retransmissions for $\alpha = 10^{-2}$.

We analyze the probability γ that two nodes are able to exchange keys without having to retransmit any packets. A similar analysis can be done for more elaborate retransmission schemes. For the basic DH scheme we have $\gamma_{dh} = (1-\epsilon)^4$. Let the probability of two nodes sharing keys be denoted by P_S, the probability that a successful key exchange occurred by P_x and let $P_B = P(B \in \mathcal{N}(t))$. Also let the complement of the first two events be denoted by $P_{\overline{S}}$ and $P_{\overline{B}}$. Let $P_S = 1-\alpha$, $P_B = 1-\beta$ and $P_X = (1-\epsilon)^4$. In our protocol, the probability that A is able to share a secret with B without the need for retransmissions is given by

$$\begin{aligned}\gamma &= P_S[P_B + P_{\overline{B}}P_X] + P_{\overline{S}}P_X \\ &= (1-\alpha)[(1-\beta)+\beta(1-\epsilon)^4] + \alpha(1-\epsilon)^4 \\ &= (1-\epsilon)^4(\alpha + (1-\alpha)\beta) + (1-\alpha)(1-\beta).\end{aligned}$$

As expected, when nodes do not share keys ($\alpha \to 1$) or are not aware of any shared keys ($\alpha \to 0$, $\beta \to 1$), γ reduces to the DH case. On the other hand, when $\alpha \to 0$ and $\beta \to 0$, $\gamma \to 1$. Fig. 4 shows the values of γ for $\alpha = 10^{-2}$ and varying values of β. We can see that γ decays much slowly for small values of β, collapsing with the DH case when $\beta = 1$. The plot shows that our scheme is fairly robust to ϵ for small values of β, meaning that if the RSU is able to inform a large enough number of vehicles, we can compensate for the consequences of channel errors. This is particularly useful in an unpredictable environment such as a VANET, where many packet losses occur sporadically due to obstacles in signal propagation.

V. Modeling and Simulation

Results from the previous section depend on a timely bootstrap of the system, which we assess through computer simulations. Focusing on urban environments, we used the STRAW mobility model [11] to simulate vehicular mobility on a 27 km^2 area of downtown Pittsburgh, PA, USA, characterized by a combination of Manhattan-like orthogonal and irregularly shaped intersections. We present results comprising a vehicle density

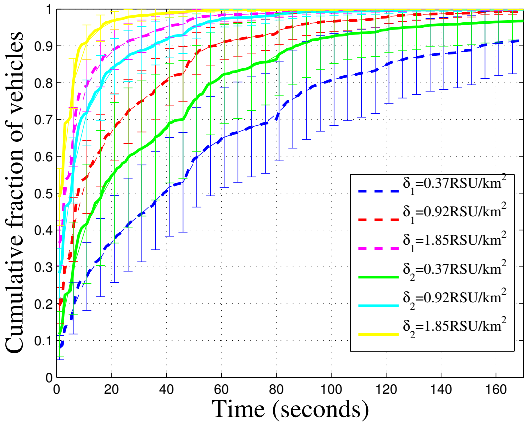

Fig. 5. Key dissemination time for varying RSU densities. Nodes are allowed to request keys in one hop (dashed lines) and multi-hop (solid lines). The vehicle density is $\rho = 10$ vehicles/km^2.

of $\rho = 10$ vehicles/km^2, which can be thought of as a sparse vehicular network. RSUs are randomly deployed with densities of 0.37, 0.92, and 1.82 RSUs/km^2. We ran 50 simulations per scenario. Each simulation run was 270 seconds, with a 100 second warm-up period for the mobility model. With respect to the communication model, since we are interested in system-level performance of our key distribution protocol, we consider a unit-disk wireless model of 150 meters radius for vehicle-to-vehicle (V2V) communications and 300 meters radius for vehicle-to-infrastructure (V2I) communications. It has been shown that, for appropriate radius, disk models mimic the shadow fading models well on a system-level [12]. Different transmission ranges were selected for V2V and V2I links based on recent experimental studies reported in [13] and [14], which showed that the RSUs placed on elevated positions above the intersections are less prone to shadowing loss, particularly from other obstructing vehicles. The parameters of our protocol are set to $t = 10$ seconds and $x = 5$.

We recall our scheme allows nodes to request keys through one-hop (direct communication with RSU) or multi-hop communications (broadcast). In Fig. 5, for varying RSU densities, we plot the cumulative fraction of vehicles that receive their keys within a given time. The dashed lines represent the case of one-hop and solid lines the case of multi-hop. The figure shows that key dissemination time in the multi-hop case is almost immediate. On the other hand, the one-hop case requires a high RSU density to achieve a timely bootstrap. Multi-hop communication at 0.92 RSUs/km^2 achieves a similar performance as single-hop at 1.82 RSUs/km^2. Simulations also confirm that increasing the vehicular density speeds up key dissemination considerably in the multi-hop case, while having almost no impact in one-hop case.

In addition, we analyze the percentage of secure paths that are immediately available for communications, i.e., when two nodes meet for the first time. A path between two nodes is considered secure if and only if each link of the path is secure. Note that this definition is directed, i.e., a secure path from A to B does not necessarily imply a secure path from B to A. Table I shows the percentage of secure paths of minimum distance as a function of the path length. We can observe that when vehicles request keys directly from the RSU, the percentage of secure connections is low whereas in the multi-hop case these values are higher. This is due to the fact that vehicles take more time to obtain their keys, and therefore when vehicles meet for the first time, they do not possess a ring of keys. When increasing the RSU density we observe an increase in the percentage of secure connections for both cases. These percentages can be considered estimates for the β parameter of the reliability analysis present in Section IV.

TABLE I
PERCENTAGE OF SECURE PATHS OF LENGTH L FOR $\rho = 10$ VEH/KM^2.

L	One-hop to RSU			Multi-hop to RSU		
	δ_1 = 0.37	δ_1 = 0.92	δ_1 = 1.82	δ_2 = 0.37	δ_2 = 0.92	δ_2 = 1.82
1	46.20%	67.41%	85.33%	60.30%	82.18%	94.18%
2	41.29%	63.60%	83.25%	58.50%	81.65%	94.45%
3	38.82%	62.04%	82.17%	58.14%	82.07%	94.71%
4	40.52%	63.91%	82.55%	61.29%	84.18%	95.27%
≥ 5	36.73%	65.34%	84.20%	65.21%	88.78%	96.80%

VI. DISCUSSION

In this section we discuss several aspects related to specific security issues in vehicular ad-hoc networks that can influence the correct operations of the proposed protocol.

A. Node compromise

As in any other ad-hoc network, the nodes of a vehicular network can be compromised (e.g., a vehicle can be stolen). Thus, efficient key revocation mechanisms must ensure that compromised nodes do not impair network security. In particular, with respect to random key distribution schemes, several techniques can be used. A centralized approach can be used, where a base station (in our case an RSU) broadcasts revocation messages to all nodes that need to remove copies of the revoked keys. The drawback of such approach is a single point of failure of the revocation scheme. Additionally, this approach involves the broadcast of messages over long distances, which might result in an undesirable communication overhead. On the other hand, key revocation can be performed in a distributed fashion. Such an approach is taken in [15] in the context of sensor networks and could be extended to our protocol for vehicular networks. Note that, since public keys from the revoked nodes are known, we can propagate the information from revoked nodes to other regions controlled by different CAs.

Although we assume that RSUs are tamper-proof, it is always possible to revoke all the keys provided by an RSU. In case an RSU is compromised, the CA should provide a new pool of keys to all RSUs that are not compromised from which vehicles will be able to obtain new keys. Moreover, vehicles need to be informed of the existence of the compromised RSUs (e.g., by broadcast of a revocation message to all vehicles).

B. Operating Across Boundaries

Since the key space is independently partitioned over a geographical space, a mechanism that ensures vehicles can communicate with vehicles controlled by other CAs is required. This can be achieved by considering parallel key spaces that address these geographical boundaries. The key pools can be coordinated among the different CAs, and vehicles that require communication between independent CAs should request a set of keys from this pool. This mechanism would operate much as a roaming service to provide keys to every possible geographic region.

VII. Conclusions

We proposed a probabilistic key distribution scheme as a mechanism for ensuring secure communication in VANETs. We show that a secure connection can be established with high probability for reasonably small key rings. Leveraging on network infrastructure, we increased the reliability of key exchange. We compared the robustness of our scheme to that of a standard Diffie-Hellman key agreement under an end-to-end erasure model, showing that our scheme requires fewer retransmissions. The main advantage of our protocol is the reduced need to invoke public-key security mechanisms. Moreover, its distributed nature alleviates the burden of a complex security infrastructure. The scheme is robust to topology changes and link failures. Furthermore, our solution preserves long term privacy since there exists no link between the keys assigned by trusted nodes that serve different geographic regions. It also prevents man-in-the-middle attacks as the keys used to share a secret are already known by the nodes and issued by authorized entities. Our future work targets similar schemes in the presence of trusted mobile nodes.

Acknowledgements

The authors would like to thank the anonymous reviewers for their comments that helped improve the manuscript.

References

[1] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, April 2007.

[2] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," in *Proc. of the ACM Workshop on Hot Topics in Networks*, November 2005.

[3] A. Weimerskirch, J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, *VANET Vehicular Applications and Inter-Networking Technologies*. Wiley, December 2009, ch. Data Security in Vehicular Communication Networks.

[4] C. Olaverri-Monreal, P. Gomes, R. Fernandes, F. Vieira, and M. Ferreira, "The See-Through System: A VANET-enabled assistant for overtaking maneuvers," in *Proceedings of the IEEE Intelligent Vehicles Symposium*, June 2010, pp. 123 –128.

[5] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, "Data aggregation and roadside unit placement for a vanet traffic information system," in *Proceedings of the fifth ACM International Workshop on VehiculAr Inter-NETworking*, ser. VANET '08, 2008, pp. 58–65.

[6] O. K. Tonguz and M. Boban, "Multiplayer games over vehicular ad hoc networks: A new application," *Ad Hoc Networks*, vol. 8, no. 5, pp. 531 – 543, 2010.

[7] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, NY, USA: John Wiley & Sons, Inc., 1995.

[8] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 41–47.

[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 communications: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, November 2008.

[10] M. Boban, T. Vinhoza, M. Ferreira, J. Barros, and O. Tonguz, "Impact of vehicles as obstacles in vehicular ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 1, pp. 15 –28, January 2011.

[11] D. R. Choffnes and F. E. Bustamante, "An integrated mobility and traffic model for vehicular wireless networks," in *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, 2005, pp. 69–78.

[12] R. Meireles, M. Ferreira, and J. Barros, "Vehicular connectivity models: From single-hop links to large-scale behavior," in *Proc. of the 70th IEEE Vehicular Technology Conference VTC2009-Fall*, September 2009.

[13] A. Paier, R. Tresch, A. Alonso, D. Smely, P. Meckel, Y. Zhou, and N. Czink, "Average downstream performance of measured ieee 802.11p infrastructure-to-vehicle links," in *Communications Workshops (ICC), 2010 IEEE International Conference on*, may 2010, pp. 1 –5.

[14] R. Meireles, M. Boban, P. Steenkiste, O. K. Tonguz, and J. Barros, "Experimental study on the impact of vehicular obstructions in VANETs," in *IEEE Vehicular Networking Conference (VNC 2010)*, Jersey City, NJ, USA, December 2010, pp. 338–345.

[15] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, pp. 233–247, 2005.