Low-complexity secret key distribution for Vehicular Networks

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 makes use of spatial and temporal correlation generally present in these types of networks. The scheme alleviates the burden of traditional public-key infrastructures. By allowing roadside units to help neighboring nodes sharing secret keys, secure communication is immediately possible between these vehicles with high probability. Our results indicate that high reliability and short key dissemination time can be achieved with low complexity.**

I. Introduction

The advances in vehicular and communication technologies have paved the way to the introduction of vehicular ad-hoc networks (VANETs), where vehicles are able to communicate between themselves and also with existing infrastructure, commonly addressed to as road-side units (RSUs). The main challenges introduced by VANETs are mainly related to vehicular mobility and the surrounding environment. For instance, the mobility patterns of vehicles tend to create pairwise connections of short duration. Consequently, the topology of the network is constantly changing. Mobility also impacts signal propagation. Adding, the fact that the environment consists of many obstacles to signal propagation, leads to an with an increase in the experienced error rate. Moreover, in many cases, hundreds of vehicles may be operating in a confined space, increasing interference and medium contention.

Clearly, VANETs come with their own security issues. Any vehicle can inject bogus information in the network, or try to disrupt network services (spreading false information or jamming communications). On the other hand, since vehicles broadcast their messages, anyone can overhear these messages and use them to their own benefit. Note that messages exchanged in a VANET have different roles, thus requiring different security measures. For instance, securing safety messages requires a scheme that would privilege authentication over confidentiality [1] (the content of the message is not particularly sensitive and may interest multiple users, while the legitimacy of the source is important). 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. The main idea is to have trusted authorities that equip vehicles with private and public key pairs as well as certificates. This allows mutual authentication to take place without involving a server. That being said, a large number of VANET applications and services may depend on confidential data transmission (e.g., [4]). If two vehicles wish to communicate securely, it is required that the data they transmit is encrypted. In this case, the standard course of action is to use PKC in order to establish a secret key and then use symmetric encryption to encrypt the data. In particular, the IEEE 1609.2 standard specifies the Elliptic Curve Integrated Encryption Scheme (ECIES) for PKC [3], which is based on Diffie-Hellman key agreement. However, there may exist several drawbacks in the use of such schemes. First, they operate in a pairwise basis, meaning that for each pair of vehicles that wish to establish a secure session, they both have to run the key agreement scheme. Second, these schemes generally involve several rounds of communication. One of the users needs to send his public key and the other user needs to send a message containing the shared secret. Users also need to also acknowledge the received messages, in order to know if the key agreement protocol finished successfully. Third, in dense networks, the overhead of message transmission and signature verification can be prohibitive [1].

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 [5]. Therefore, it is crucial that the key agreement protocol makes use of the least possible interaction between users to minimize the overall delay of the procedure, as well as maximizing the probability of success and reduce medium contention. In this context, we provide an alternative solution to the problem of key management in vehicular networks using the concept of randomized key pre-distribution (RKPD) [6]. In RKPD, nodes are loaded with a random set of keys, drawn from a larger pool of keys, which they advertise to their neighbors by broadcast the key identifiers. If nodes share one or more keys, then they use them as a shared secret. Since in RKPD keys are computed from the common information possessed by nodes, interaction between users is minimized.

Our main contributions are two-fold. First, we propose a key distribution protocol that enables vehicles to establish

This work was supported in part by the Fundação para a Ciência e Tecnologia (FCT), under the project VTL (PTDC/EIAC-CCO/118114/2010).

secure pairwise connections with arbitrarily high probability of success and low communication complexity. This protocol, initially presented in [7], exploits spatially bounded communication patterns that are present in VANETs by using existing infrastructure to advertise the common keys between vehicles that are possibly near each other. Second, we provide an analysis of effectiveness of establishing a secure connection, as well as its robustness with respect to eavesdropping attacks. We also show that our scheme requires less transmissions than standard schemes based on PKC. 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. Section II addresses the system setup and describes the proposed protocol. In Section III we analyze the security and reliability aspects of our protocol. Simulations are carried out in Section IV, to understand the secure network connectivity. Section V concludes the paper.

II. Key Distribution Scheme for VANETs

Before describing the protocol, it should be clear who are the network participants. We assume that VANETs are composed by mobile nodes (vehicles) and static nodes (RSUs). Vehicles are equipped with on-board units (OBUs) and IEEE 802.11p radios. We also assume the existence of trusted certification authorities (CAs), which are responsible for issuing at least one pair of public-private keys and the corresponding certificates. However, the details on how the CAs operate do not interest us (we will only need the keys / certificates for authentication purposes). RSUs play a central role in our key distribution scheme. These are infrastructure-based devices located next to the road, and therefore provide coverage within a given radio range. In the context of our protocol, RSUs will be the nodes that enable key dissemination, hence, we assume that they are permanently connected to CAs.

A. Key Distribution Protocol

The basic principle behind our key distribution protocol relies on RKPD [6]. However, unlike RKPD, keys are not pre-loaded into vehicles, but rather vehicles request these keys to RSUs. Thus, whenever an RSU receives a message from a vehicle, say V, requesting keys, it draws a ring of k keys out of a pool of N keys, and sends the node this set of keys, denoted $\mathcal{K}_V$, together with their identifiers. Note that this procedure should be made secret from all other network participants. Therefore, when requesting keys, a node should also send its public key to the RSU. On the other hand, the RSU's response should be encrypted with the node's public key. At this point, the node requesting the keys only knows its own keys. If two nodes wished to communicate securely, each node would need to broadcast their key identifiers to find the common keys. However, we know that the communication patterns in VANETs are generally local. Therefore, we can make use of the infrastructure to inform incoming nodes about their possible neighbors, as well as informing the possible neighbors about incoming nodes. Hence, upon key request of some vehicle V, the RSU sends to V a list of identifiers of the common keys shared by him and the set $\mathcal{N}(t)$ of vehicles that have contacted the RSU at most t seconds ago. By exploiting time correlation, 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. On the other hand, 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 (spatial correlation). 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.

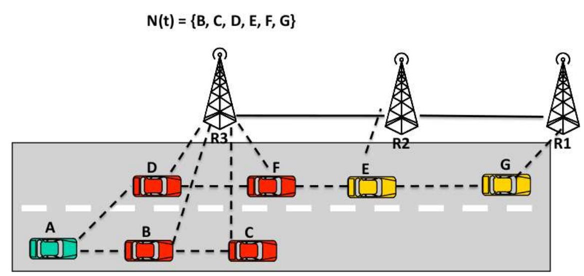

Fig. 1. Example of the key request procedure.

Note that the protocol can support both one-hop key request (meaning a node can only request keys if its within radio range of an RSU) or multi-hop key request. The former approach limits the number of messages flooded in the network. On the other hand, it requires higher RSU density 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. The nature of the information flowing in the network feed nodes with asymmetric information. In particular, the node that wishes to start secure communication might not be aware of the receiver's keys because that information might not have reached him yet. In this case, nodes will have to broadcast their key identifiers to find common keys, i.e., fall-back to the standard RKPD scheme. On the other hand, nodes might actually not share any common keys. In this case, they fall-back to one of the standard key agreement approaches. If in both these cases there s nothing to be gained in terms of saving transmissions, the same is not true when nodes actually share keys are are aware of it. In this case, they already possess a shared secret and do not need to exchange further information. To increase the probability of this latter case, we can increase the protocol parameters t and x, informing a much larger set of vehicles. The trade-off is bandwidth use, as the size and number of transmitted messages increases with t and x.

III. Security and Reliability Analysis

In this work we focus on data confidentiality and, therefore, we assume that our attacker is passive. 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. Our goal is keep the contents of transmitted messages secret to all users, except the authorized ones. In order for an eavesdropper to successfully attack a link he has to possess all the keys used to compute the shared secret [6], i.e., we assume that the eavesdropper in unable to break the underlying cipher. In this context, a group of colluding eavesdroppers can be seen as a single eavesdropper with access to a larger set of keys.

A. Probability of Secure Connection

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 $0 \leq |\mathcal{E}| = k' \leq N$. The probability that two legitimate nodes share exactly s keys, $0 \leq s \leq k$, is given by

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

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

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

Naturally, if users share no keys, then an outage occurs. We are interested in keeping the outage probability vanishingly small for the chosen parameters, such that colluding eavesdroppers are not able to compromise the system.

Fig. 2 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 only has a probability $P_{outage} = 10^{-6}$ of compromising a link, thus showing the system is fairly robust.

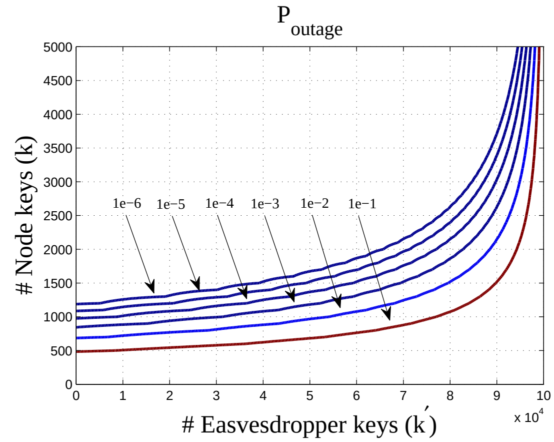

Fig. 2. Outage probability for $P = 100000$. Lines are for a probability of outage of respectively $P_{outage} = [1e-1, 1e-2, \ldots, 1e-6]$.

B. Reliability

As we mentioned in previous sections we are also interested in minimizing the number of transmissions involved in key agreement. We compare the efficiency of our scheme to that of a basic Diffie-Hellman (DH) key agreement scheme [8] assuming an end-to-end erasure model, where packets are lost with probability ϵ. Like, the ECIES, the DH scheme involves a total of four transmission (including acknowledgments). On the other hand, our protocol requires no transmission if nodes share common keys and are aware of them, or it requires the same number of transmissions as DH if this is not the case. Let γ be the probability that two nodes are able to exchange keys without having to retransmit any packets. 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

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

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. 3 plots γ for $\alpha = 10^{-2}$ and varying values of β. We can see that γ decays slowly for small values of β, collapsing with DH 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. As mentioned in Section II, we can tweak the parameters t and x of our protocol, leading to different values for α and β. This means that we can tune our protocol to reduce the number of transmissions by having RSUs informing the right amount of neighboring vehicles.

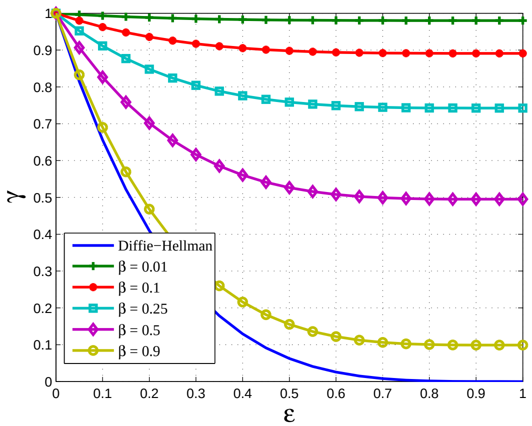

Fig. 3. Probability that two nodes are able to share a secret without retransmissions for $\alpha = 10^{-2}$.

IV. Modeling and Simulation

To obtain the aforementioned efficiency gains, a timely bootstrap of the system needs to be guaranteed. In this section we present simulation results that show this is achievable. We used the STRAW mobility model [9] to simulate vehicular mobility on a 27 km^2 area of downtown Pittsburgh, PA, USA. Each experiment was repeated 50 times, with a simulation time of 270 seconds. The considered channel model was a unit-disk wireless model of 150 meters radius for vehicle-to-vehicle (V2V) communications and 300 for vehicle-to-infrastructure (V2I) communications. For an appropriate radius, disk models mimic the shadow fading models well on a system-level [10]. Different transmission ranges were selected for V2V and V2I links based on experimental studies reported in [11] and [12], which showed that the RSUs placed on elevated positions above the intersections are less prone to shadowing loss. The parameters t and x are set to 10 seconds and 5. We use a vehicle density of $\rho = 10$ veh./km^2 (sparse network), with RSUs randomly deployed with several densities. In Fig. 4 we plot the cumulative fraction of vehicles that receive their keys within a given time. The dashed lines represent one-hop based key request and the solid lines represent of multi-hop case. The results confirm that for one-hop key request, a high RSU density is required. On the other hand, when key requests can be done through multi-hop, we only require sparsely deployed RSUs. Moreover, with increasing vehicle densities, key dissemination speeds up considerably.

V. 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

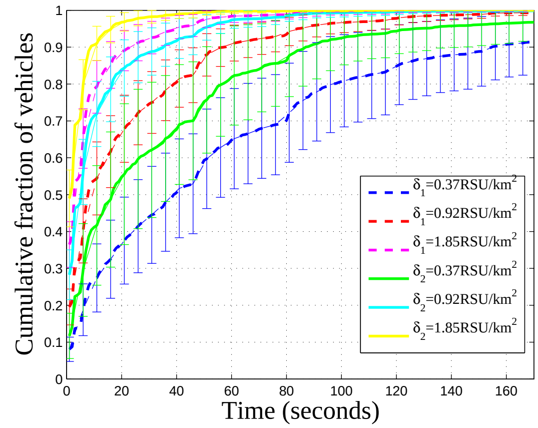

Fig. 4. Key dissemination time for varying RSU densities. Nodes are allowed to request keys in one hop (dashed lines) and multi-hop (solid lines). The vehicle density is $\rho = 10$ vehicles/km^2.

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.

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*, Nov. 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 *IEEE Intelligent Vehicles Symp.*, June 2010, pp. 123 – 128.

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

[6] 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.

[7] J. Almeida, S. Shintre, M. Boban, and J. Barros, "Probabilistic Key Distribution in Vehicular Networks with Infrastructure Support," in *IEEE Globecom*, December 2012.

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

[9] D. R. Choffnes and F. E. Bustamante, "An integrated mobility and traffic model for vehicular wireless networks," in *2nd ACM International Workshop on Vehicular Ad-hoc Networks*, 2005, pp. 69–78.

[10] 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.

[11] 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.

[12] 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.