

DESCRIPTION

Probabilistic Key Distribution in Vehicular Networks with Infrastructure Support

Technical field

[0001] Probabilistic key distribution protocol for vehicular network that alleviates the burden of traditional public-key infrastructures, wherein 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, providing high reliability and short dissemination times that can be achieved with low complexity.

Background art

[0002] 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.

[0003] 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].

[0004] 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 fallback to a simple digital signature scheme is ensured.

[0005] 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.

[0006] 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.

Summary

[0007] The disclosure comprises a method of key distribution by trusted nodes for a vehicular ad hoc network, VANET, wherein said vehicular ad hoc network is composed of nodes, a node being either a mobile vehicle node equipped with an on-board unit or a static road-side unit node, herewith referred respectively as vehicle nodes and RSU nodes, wherein said RSU nodes have a permanent connection to a certificate authority, CA, said CA being responsible for a specific geographic region in which the VANET is comprised and said CA acting as the root of trust for the VANET, and wherein the VANET nodes have at least one pair of public-private keys and the corresponding certificates, issued by said CA, wherein said method comprises the steps of:

- each vehicle node, on entering said specific geographic region, requests a set of keys from an RSU node that is within range and within that region, either
 - by direct communication, or
 - by through multi-hop communication,wherein said vehicle node sends a key request to said RSU, said request including the vehicle node public key;
- said RSU node sends said vehicle node a set of private keys, selected from a pool of private keys available to the RSU node, said set of keys being encrypted with the vehicle node public key, wherein said set of private keys also includes a key identifier for each private key in said set;
- said RSU node sends said vehicle node a list with the key identifiers of the private keys shared by said vehicle node and the other vehicle nodes that have most recently contacted said RSU for a predetermined period of time;

- said RSU informs the VANET nodes, within a neighborhood of a predetermined number of hops from said RSU, of the presence of said vehicle node and of the identifiers of keys obtained by said vehicle node;

such that two vehicle nodes are able to immediately establish a secure connection if there are shared keys between those two vehicles, without further interaction, by deriving a new shared secret which is a cryptographic hash function of the keys shared by said two nodes.

[0008] An embodiment, wherein a sender node which is interested in communicating with a receiver node, if said sender node does not know the private keys held by the receiver node, comprises the step of both nodes broadcasting the key identifiers of the private keys held by each node, such that if there are shared keys then two nodes are then able to establish a secure connection, without further interaction, by deriving a new shared secret which is a cryptographic hash function of the keys shared by said vehicle node and one of the other vehicle nodes.

[0009] In an embodiment, wherein if there are not shared keys between the two nodes, then the two nodes will establish a shared secret via standard PKC methods.

[0010] In an embodiment, wherein if an RSU node or nodes are compromised, said method comprises the steps of:

- the CA provides a new pool of keys to all RSU nodes that are not compromised, from which said pool of keys the vehicle nodes will then be able to obtain new keys;
- the vehicle nodes are informed of the existence of the compromised RSU node or nodes.

[0011] In an embodiment, the private key identifiers are sequential IDs attributed as the private keys are generated.

[0012] In an embodiment, for key distribution spanning multiple independent CA's, each CA with a predetermined geographical area, the pool of private keys available to each RSU node is unique to a partitioned key space corresponding to the geographical area of each independent CA.

[0013] In an embodiment, for key distribution spanning multiple independent CA's, each CA with a predetermined geographical area, the pool of private keys available to each RSU node comprises an additional key space that is parallel to said CA's and is thus shared by all CA's.

[0014] In an embodiment, for key distribution spanning multiple independent CA's, each CA with a predetermined geographical area, said additional key space is made available by the RSU nodes only to vehicles that require communication between independent CAs.

[0015] An embodiment, for a vehicle node on moving from a first CA geographic region to a second CA geographic region, comprises the following steps:

- before leaving said first CA geographic region, said vehicle node requests a set of keys from an RSU node that is within range and within that first CA region, indicating that those requested keys are for said second CA geographic region;
- said RSU node then sends the vehicle node request to the first CA for a set of keys that can be used within the region controlled by the second CA;
- the first CA forwards the vehicle node request to the second CA;
- the second CA responds with a set of keys that can be used within the region controlled by the second CA with the respective list of identifiers which are sent to to the vehicle node encrypted with the vehicle node public key;

such that such the vehicle node will be able to immediately establish a secure connection with any node in said second CA geographic region by deriving a new shared secret which is a cryptographic hash function of the keys shared by the two nodes.

[0016] In an embodiment, for a vehicle node on moving from a first CA geographic region to a second CA geographic region, said RSU node is a RSU border node of the first CA geographic region.

[0017] The disclosure also comprises a device for key distribution by trusted nodes for a vehicular ad hoc network, VANET, wherein said vehicular ad hoc network is composed of nodes, a node being either a mobile vehicle node equipped with an on-

board unit or a static road-side unit node, herewith referred respectively as vehicle nodes and RSU nodes, wherein said RSU nodes have a permanent connection to a certificate authority, CA, said CA being responsible for a specific geographic region in which the VANET is comprised and said CA acting as the root of trust for the VANET, and wherein the VANET nodes have at least one pair of public-private keys and the corresponding certificates, issued by said CA, wherein each node comprises a data processing module configured to carry out the method of any one of the previous embodiments.

[0018] The disclosure also comprises a computer readable data carrier comprising the computer program instructions adapted to perform the method of any of the previous embodiment methods when said program is run on a data processor.

Disclosure of the invention

[0019] The proposed probabilistic key distribution scheme can act as a mechanism for ensuring secure communication in VANETs. The present protocol ensures that a secure connection can be established with high probability for reasonably small key rings. Leveraging on network infrastructure, the number of (re)transmissions required by the key exchange protocol can be reduced when compared to that of a standard Diffie-Hellman key agreement under an end-to-end erasure model. The main advantages of the protocol here proposed are: i) reduction of the need to invoke public-key security mechanisms, ii) reduction of the amount of messages exchanged during the secret sharing procedure and iii) reduced complexity of security infrastructure. The scheme is robust to topology changes and link failures. Furthermore, the present 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. The present disclosure is applicable to similar schemes in the presence of trusted mobile nodes.

[0020] The proposed method provides 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.

[0021] Main contributions are as follows:

- **Key distribution protocol:** A probabilistic key distribution protocol that enables vehicles to establish secure pairwise connections with arbitrarily high probability of success and low communication complexity is proposed. 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:** The effectiveness of establishing a secure connection is analyzed, as well as its robustness with respect to eavesdropping attacks. 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.

[0022] This document is organized as follows. It will be provided a discussion on the existing solutions to the problem of secret key sharing in vehicular networks. It will also be presented the method of probabilistic key-distribution. The system setup and proposed protocol are described. The security of the scheme is analyzed. The model and environments under which the performance of the scheme is analyzed are described. It is also discussed several operational aspects of the proposed scheme.

[0023] The following pertains to the Key Distribution Scheme for VANETs and its network Model.

[0024] A VANET is composed of nodes, which can be mobile (vehicles) or static (road-side units or RSUs). A VPKI is assumed to be 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. RSUs are considered to have a permanent connection to some CA. Vehicles are equipped with on-board units (OBUs) and IEEE 802.11p radios. No assumptions are made with respect to 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).

[0025] The following pertains to the Key Distribution Protocol.

[0026] 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. Users can 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.

[0027] More precisely, let vehicle $\mathbf{V}$ send a key request message to an RSU with its public key $\mathbf{K}_V$. The RSU draws a ring of $\mathbf{k}$ keys out of a pool of $\mathbf{N}$ keys, and sends the vehicle node the set of keys $\mathbf{K}_V$ (encrypted with the vehicle node's public key), along with the respective identifiers. Additionally, the RSU sends to vehicle node $\mathbf{V}$ a list of identifiers of the common keys shared by $\mathbf{V}$ and the set $\mathbf{N}(\mathbf{t})$ of vehicles that have contacted the RSU at most $\mathbf{t}$ seconds ago. By exploiting this information about nearby vehicles, vehicle $\mathbf{V}$ will be able to immediately establish a secure connection

with the vehicles in $\mathbf{N}(t)$ without further interaction, as long as they share some keys. The RSU also informs its x-hop neighborhood, $\mathbf{N}_x$, about the presence of vehicle $\mathbf{V}$, broadcasting the identifiers of keys attributed to vehicle $\mathbf{V}$. This allows the vehicles in $\mathbf{N}_x$ to have fresh information about incoming vehicles that are geographically close. Suppose that two vehicle nodes share s keys, $k_1, \dots, k_s$, with $s > 0$. They secure the communication link by deriving a new shared secret $\mathbf{K} = f(k_1, \dots, k_s)$, where $f(\cdot)$ is a cryptographic hash function.

[0028] Fig.1 illustrates the key dissemination procedure. Here, vehicle node $\mathbf{A}$ requests a set of keys to RSU $\mathbf{R}_3$. Suppose this RSU has been contacted by all the nodes in the figure in the last t seconds, i.e. $\mathbf{N}(t) = \{\mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}, \mathbf{F}, \mathbf{G}\}$. RSU $\mathbf{R}_3$ will send vehicle node $\mathbf{A}$ a list of all the key identifiers that vehicle nodes $\mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}, \mathbf{F}$ and $\mathbf{G}$ have in common with vehicle node $\mathbf{A}$. Now consider that RSU $\mathbf{R}_3$ will inform its 1-hop neighborhood, $\mathbf{N}_1 = \{\mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{F}\}$, about the keys assigned to vehicle node $\mathbf{A}$, i.e., RSU $\mathbf{R}_3$ will send a message to vehicle nodes $\mathbf{B}, \mathbf{C}, \mathbf{D}$ and $\mathbf{F}$ with the key identifiers from vehicle node $\mathbf{A}$. Assuming that vehicle node $\mathbf{A}$ shares keys with these nodes, it can immediately communicate securely with the set of vehicle nodes $\{\mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}, \mathbf{F}, \mathbf{G}\}$ without further interaction, while at the same time the set of vehicle nodes $\{\mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{F}\}$ can also immediately communicate securely with vehicle node $\mathbf{A}$ without further interaction.

[0029] 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 fallback to one of the standard key agreement approaches.

[0030] 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.

[0031] The following pertains to security analysis and its threat model.

[0032] The concern in this work is to ensure means for confidential data transmission, and therefore it is assumed 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, the attacker is a passive entity which tries to eavesdrop on transmitted messages. Although passive attacks impose fewer risks to the safety of the vehicular network users, in general, they are also more difficult to detect than active attacks.

[0033] The messages exchanged over the wireless links are assumed to be encrypted – in particular, after bootstrapping the protocol, using the newly derived key. 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 – in particular, after bootstrapping the protocol, the new derived key. 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.

[0034] The following pertains to the probability of secure connection.

[0035] The key used to encrypt the communication link (after bootstrap) 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.

[0036] 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 $0 \leq |\mathcal{E}| = k' \leq N$. As the presence of this eavesdropper is not known, one does not know which keys are compromised. Nevertheless, the amount of keys required to compromise the security of pairwise

connections can be estimated. Let $P(|\mathcal{K}_A \cap \mathcal{K}_B| = s)$ denote the probability that two legitimate nodes share exactly s keys, $0 \leq s \leq k$. Then

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

[0037] 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

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

[0038] 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

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

[0039] There exists a trade-off between P_S and P_{outage} . On one hand, it is required 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, the outage probability should be kept 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 only has a probability $P_{\text{outage}} = 10^{-6}$ of compromising a link, thus showing the system is fairly robust.

[0040] The following pertains to the reliability.

[0041] Analyzing the reliability of a key distribution scheme in a dynamic scenario such as a vehicular network is a complex task. Consider 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 .

[0042] Assume that node **A** wishes to share a secret with node **B**. In the DH protocol, each node transmits a message prior to computing a shared secret. Additionally, the two nodes must acknowledge the reception of both packets, which gives four transmissions in total. In the proposed 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 fallback to the DH scheme.

[0043] The reduction on the number of transmitted messages can be analyzed through 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 the aforementioned probability is given by $\gamma_{\text{dh}} = (1 - \epsilon)^4$. 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 $P_B = P(\mathbf{B} \in \mathcal{N}(\mathbf{t}))$. Also let the complement of the first two events be denoted by $P_{\bar{s}}$ and $P_{\bar{B}}$. Let $P_s = 1 - \alpha$, $P_B = 1 - \beta$ and $P_x = (1 - \beta)^4$. In the proposed method, the probability that **A** is able to share a secret with **B** without the need for retransmissions is given by

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

[0044] As expected, when nodes do not share keys ($\alpha \rightarrow 1$) or are not aware of any shared keys ($\alpha \rightarrow 0$, $\beta \rightarrow 1$), γ reduces to the DH case. On the other hand, when $\alpha \rightarrow 0$ and $\beta \rightarrow 0$, $\gamma \rightarrow 1$. Fig. 4 shows the values of γ for $\alpha = 10^{-2}$ and varying values of β . γ decays much slowly for small values of β , collapsing with the DH case when $\beta = 1$. The plot shows that the 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, one 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.

[0045] In the following, several aspects related to specific security issues in vehicular ad-hoc networks, that can influence the correct operations of the proposed protocol, are discussed.

[0046] The following pertains to node compromise.

[0047] 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 (e.g. 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 vehicular networks. Note that, since public keys from the revoked nodes are known, the information regarding revoked nodes can be propagated to other regions controlled by different CAs.

[0048] 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. Prior keys obtained from the compromised RSU should also be revoked and vehicle informed of the compromise (e.g., by broadcast of a revocation message to all vehicles).

[0049] The following pertains to operating across boundaries.

[0050] 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.

[0051] This roaming service can also be used to assign keys to vehicles that are entering a certain CA geographic region without the need to communicate with an RSU that is within that CA region for requesting keys specific to that CA geographic region.

[0052] Consider (see fig. 6) that a vehicle in a geographic region controlled by CA 2 wishes to communicate with another vehicle that is located within the geographic region covered by CA 3. Then, the vehicle must send a request message to an RSU requiring a set of keys for a new key space, which holds the keys to be used for vehicles communicating between the regions defined by CA 2 and CA 3. These keys are independent from the keys used within each region. The key establishment procedure can now take place as described in the text pertaining to the key distribution protocol.

[0053] On the other hand, consider a vehicle that is moving from a region covered by CA 2 onto the region covered by CA 3. Then, this vehicle can proactively request an RSU within this CA2 region for keys for the new region CA3 to which he is moving towards. This request should be preferably done to RSUs that are near the border of the region. The RSU then requests CA 2 for a set of keys that can be used within the

region controlled by CA 3. CA 2 forwards this request to CA 3, which answers with a set of keys and a list of identifiers encrypted with the vehicles public key. The vehicle can now use these keys immediately once he reaches the region controlled by CA 3.

[0054] VANET is commonly defined as a Vehicular Ad-Hoc Network which is a class of wireless networks composed of mobile and static nodes. Mobile nodes are nodes whose geographic position changes according to time at different velocities. The most common form of mobile nodes are vehicles equipped with wireless interfaces of homogeneous or heterogeneous technologies. Vehicles can either be private or belong to a public transportation system. Other mobile nodes can also be a part of the network such as mobile end-user devices (these are generally characterized by slow mobility). Static nodes do not change their geographic position in time. They can be a part of a specialized network infrastructure such as road-side units (or road-side equipment) that supports vehicular communication. These units can be part of private networks, controlled by network operators/service providers or part of a network controlled by a public entity, such as the government or a municipality. For example, see the reference: Vehicular Network: Techniques, Standards, and Applications. Published: April 9, 2009. Editors: Hassnaa Moustafa; Yan Zhang (Chapter 1).

[0055] Certificate Authorities (CAs) are commonly defined as entities assumed to be responsible for the certification/attribution of public/private keys that are permanently assigned to vehicles. There are two types of envisioned CAs: public authorities (such as vehicle registration authorities) or private authorities (such as car manufacturers). In the case of public authorities several types of CAs can be considered according to some geographic refinement (e.g. a CA covers vehicles within a country, state, metropolitan area, etc...). Different CAs are assumed to be cross-certified so that vehicles with keys issued by different CAs can authenticate/communicate with each other. For example, see the reference: Securing Vehicular Communications, Maxim Raya, Panos Papadimitratos, Jean-Pierre Hubaux. In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006.

[0056] VPKI, vehicular public key infrastructure, is commonly defined as an infrastructure responsible for providing a set of security services, based on public key cryptography, that support vehicular communications. Examples of services include positioning, authentication, privacy and confidentiality. They are supported by CAs which issue/certificate the cryptographic material. The VKPI is ultimately responsible for providing a robust and scalable key management scheme. For example, see the reference: Securing Vehicular Communications, Maxim Raya, Panos Papadimitratos, Jean-Pierre Hubaux. In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006.

[0057] The embodiments described may be combined. The following claims set out particular embodiments of the invention.

Brief Description of Drawings

[0058] The following figures provide preferred embodiments for illustrating the description and should not be seen as limiting the scope of invention.

[0059] **Figure 1:** Schematic representation of a first preferred embodiment of an example of the key request procedure where:

- (A) represents the vehicle requesting keys,
- (B) represents a vehicle in the network that may want to have a secure connection with A,
- (C) represents a vehicle in the network that may want to have a secure connection with A,
- (D) represents a vehicle in the network that may want to have a secure connection with A,
- (E) represents a vehicle in the network that may want to have a secure connection with A,

(F) represents a vehicle in the network that may want to have a secure connection with A,

(G) represents a vehicle in the network that may want to have a secure connection with A,

(R1) represents a Road Side Unit,

(R2) represents a Road Side Unit, and

(R3) represents a Road Side Unit to which A requests a set of keys.

[0060] **Figure 2:** Schematic representation for an embodiment of the probability of two nodes sharing a secret key not possessed by any of their d neighbors. Key pool size $P = 100000$.

[0061] **Figure 3:** Schematic representation for an embodiment of the Outage probability for $P = 100000$. Lines are for a probability of outage of respectively $P_{\text{outage}} = [1e-1, 1e-2, \dots, 1e-6]$.

[0062] **Figure 4:** Schematic representation for an embodiment of the probability that two nodes are able to share a secret without retransmission for $\alpha = 10^{-2}$.

[0063] **Figure 5:** Schematic representation for an embodiment of the 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 .

[0064] **Figure 6:** Schematic representation for an embodiment of roaming between VANETs.

Detailed description

[0065] Results from the previous section depend on a timely bootstrap of the system, which can be assessed through computer simulations. Focusing on urban environments, the STRAW mobility model [11] is used to simulate vehicular mobility on a 27km^2 area of downtown Pittsburgh, PA, USA, characterized by a combination of Manhattan-like orthogonal and irregularly shaped intersections. The results presented comprise a vehicle density 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 . For each RSU deployment density, 50 simulations were performed. Each simulation run was 270 seconds, with a 100 second warm-up period for the mobility model. The considered communication model is 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 the protocol are set to $t = 10$ seconds and $x = 5$.

[0066] The proposed 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, it is shown 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.

[0067] In addition, the percentage of secure paths that are immediately available for communications, i.e., when two nodes meet for the first time, is analyzed. 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**.

[0068] Table 1 shows the percentage of secure paths of minimum distance as a function of the path length. 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 the percentage of secure connections for both cases increases. These percentages can be considered estimates for the β parameter of the reliability analysis.

Table 1: Percentage of secure paths of length L for $\rho = 10$ vehicles /km².

L	One-hop to RSU			Multi-Hop to RSU		
	$\delta_1 = 0.37$	$\delta_1 = 0.92$	$\delta_1 = 1.82$	$\delta_2 = 0.37$	$\delta_2 = 0.92$	$\delta_2 = 1.82$
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%

[0069] The invention is of course not in any way restricted to the embodiments described and a person with ordinary skill in the art will foresee many possibilities to modifications thereof without departing from the invention as defined in the appended claims.

CLAIMS

1. Method of key distribution by trusted nodes for a vehicular ad hoc network, VANET, wherein said vehicular ad hoc network is composed of nodes, a node being either a mobile vehicle node equipped with an on-board unit or a static road-side unit node, herewith referred respectively as vehicle nodes (A, B, C, D, E, F, G) and RSU nodes (R1, R2, R3), wherein said RSU nodes have a permanent connection to a certificate authority, CA, said CA being responsible for a specific geographic region in which the VANET is comprised and said CA acting as the root of trust for the VANET, and wherein the VANET nodes have at least one pair of public-private keys and the corresponding certificates, issued by said CA, wherein said method comprises the steps of:
 - each vehicle node, on entering said specific geographic region, requests a set of keys from an RSU node that is within range and within that region, either
 - by direct communication, or
 - by through multi-hop communication,wherein said vehicle node sends a key request to said RSU node, said request including the vehicle node public key;
 - said RSU node sends said vehicle node a set of private keys, selected from a pool of private keys available to the RSU node, said set of keys being encrypted with the vehicle node public key, wherein said set of private keys also includes a key identifier for each private key in said set;
 - characterised in that it further comprises the steps of
 - said RSU node sends said vehicle node a list with the key identifiers of the private keys shared by said vehicle node and the other vehicle nodes that have most recently contacted said RSU node for a predetermined period of time;
 - said RSU node informs the VANET nodes, within a neighborhood of a predetermined number of hops from said RSU node, of the presence of said vehicle node and of the identifiers of keys obtained by said vehicle node;such that two vehicle nodes are able to immediately establish a secure connection if there are shared keys between those two vehicles, without further

interaction, by deriving a new shared secret which is a cryptographic hash function of the keys shared by said two nodes.

2. Method according to the previous claim, wherein a sender node which is interested in communicating with a receiver node, if said sender node does not know the private keys held by the receiver node, comprises the step of both nodes broadcasting the key identifiers of the private keys held by each node, such that if there are shared keys then two nodes are then able to establish a secure connection, without further interaction, by deriving a new shared secret which is a cryptographic hash function of the keys shared by said vehicle node and one of the other vehicle nodes.
3. Method according to the previous claim, wherein if there are not shared keys between the two nodes, then the two nodes will establish a shared secret via standard PKC methods.
4. Method according to any previous claim, wherein if an RSU node or nodes are compromised, said method comprises the steps of:
 - the CA provides a new pool of keys to all RSU nodes that are not compromised, from which said pool of keys the vehicle nodes will then be able to obtain new keys;
 - the vehicle nodes are informed of the existence of the compromised RSU node or nodes.
5. Method according to any of the previous claims, wherein the private key identifiers are sequential IDs attributed as the private keys are generated.
6. Method according to any of the previous claims, for key distribution spanning multiple independent CA's, each CA with a predetermined geographical area, wherein the pool of private keys available to each RSU node is unique to a partitioned key space corresponding to the geographical area of each independent CA.

7. Method according to the previous claim, wherein the pool of private keys available to each RSU node comprises an additional key space that is parallel to said CA's and is thus shared by all CA's.
8. Method according to the previous claim, wherein said additional key space is made available by the RSU nodes only to vehicles that require communication between independent CAs.
9. Method according to any of the claims 6 - 8, wherein a vehicle node on moving from a first CA geographic region to a second CA geographic region, comprises the following steps:
 - before leaving said first CA geographic region, said vehicle node requests a set of keys from an RSU node that is within range and within that first CA region, indicating that those requested keys are for said second CA geographic region;
 - said RSU node then sends the vehicle node request to the first CA for a set of keys that can be used within the region controlled by the second CA;
 - the first CA forwards the vehicle node request to the second CA;
 - the second CA responds with a set of keys that can be used within the region controlled by the second CA with the respective list of identifiers which are sent to to the vehicle node encrypted with the vehicle node public key;such that such the vehicle node will be able to immediately establish a secure connection with any node in said second CA geographic region by deriving a new shared secret which is a cryptographic hash function of the keys shared by the two nodes.
10. Method according to the previous claim, wherein the RSU node is a RSU border node of first CA geographic region.
11. Device for key distribution by trusted nodes for a vehicular ad hoc network, VANET, wherein said vehicular ad hoc network is composed of nodes, a node being either a mobile vehicle node equipped with an on-board unit or a static road-side unit node, herewith referred respectively as vehicle nodes (A, B, C, D, E, F, G) and RSU nodes (R1, R2, R3), wherein said RSU nodes have a permanent

connection to a certificate authority, CA, said CA being responsible for a specific geographic region in which the VANET is comprised and said CA acting as the root of trust for the VANET, and wherein the VANET nodes have at least one pair of public-private keys and the corresponding certificates, issued by said CA, wherein each node comprises a data processing unit configured to carry out the method of any one of the previous claims.

12. Computer readable data carrier comprising the computer program instructions adapted to perform the method of any of the claims 1-10 when said program is run on a data processing unit.