Layered and Service-Dependent Security in CSMA/CA and Slotted Vanets

Luca Pilosu*, Hector Agustin Cozzetti, and Riccardo Scopigno

Istituto Superiore Mario Boella
Via P.C. Boggio 61, 10138 Torino, Italy
{pilosu,cozzetti,scopigno}@ismb.it

Abstract. The implications and challenges of security in vehicular ad-hoc networks are huge for several reasons and, basically, for human safety effects and due to the complex and highly dynamic setting. Additionally security, being a cross-layer topic, can be managed at different layers of the network stack (e.g. at MAC-level - with encryption and authentication, at network-layer - as with IPsec, at transport-layer TLS, SSL). A rich scientific literature has addressed the issue of vanet security, however, all the proposed solutions (i) focus on a specific layer and (ii) offer either robust but not scalable solutions (such as the PKI infrastructure, hardly managed under mobility for all the nodes and services) or weak ones (at least weak if applied to human safety). For this reason, in the present paper, security for vanet is faced with a layered approach which lets envisage several solutions, properly and hierarchically differentiated for distinct services. Additionally, what introduces an even stronger novelty, the dissertation covers both CSMA/CA and slotted MAC protocols, having the latter recently encountered a certain scientific favour.

1 Security in Vehicular Ad-Hoc Networks

In vehicular ad-hoc networks (vanets), each vehicle contributes to create the network structure by establishing dynamic links to different nodes in its neighborhood. Therefore, possible vulnerabilities affecting any node in the network can dramatically lower the security level of the whole network, which does not have a pre-defined architecture (and hierarchy).

Moreover, the typical characteristics of the wireless medium make it difficult to implement strong and strict controls on the communications. The main problem is that any node within the transmission range can easily eavesdrop and participate in communications. All in all, it is early clear that security constitutes one of the main criticalities in vanets and, as such, requires a deep analysis.

Vanets are meant to support a wide range of services and each demands specific guarantees on security. For instance, safety messages include critical

* This research work has been carried out within *IoT - Piattaforma Tecnologica Innovativa per l'IoT* Project, supported by regional fundings of Regione Piemonte - Italy.

X. Zhang and D. Qiao (Eds.): QShine 2010, LNICST 74, pp. 612–622, 2011.

alerts aimed at delivering real-time life-services (including accident prevention and reactive cooperative driving): consequently they require a very high level of security - in terms of integrity, reliability and overall authentication of the network architecture. Other applications (e.g., infotainment and location-based services) can tolerate more relaxed requisites however they can benefit too from a controlled and traced access - for example for user profiling.

Finally, independently on the delivered services, also the MAC protocol itself can gain benefits from integrity and consistency checks, to infer possible misbehaving nodes – this also can be considered security-related.

As a result security can be managed at different layers of the network stack (*e.g.* MAC-level WPA2 encryption and authentication, network-layer IPsec, transport-layer TLS, SSL) - this reflects the more general attitude of security, being a cross-layer topic [4]. The most suitable solution depends on the characteristics of the application being protected, but also on the kind of the attack which has to be faced.

Concerning this point, literature shows that the effects on the network can be different if caused from internal or external, persistent or random, accidental or malicious attacks. Some of the most important attacks that can be carried on in vehicular networks are [9]:

- **jamming:** the attacker generates voluntarily interfering signals, in order to block all the communications in his transmission range;
- **poison traffic attack:** the attacker injects fake information into the network;
- **alteration traffic attack:** in this attack, the information sent regularly from other vehicles are altered and forwarded;
- **stolen identity:** the attacker personifies a different identity (e.g., a police vehicle), with the goal of propagating fake information without being caught.

So far security has been mentioned as a cross-layer and service-dependent issue. But also the underlying protocols may play a meaningful role. The emerging international standard is based on CSMA/CA (in the WAVE stack, the 802.11p standard [1] defines enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications in the licensed band of 5.9 GHz (5.85-5.925 GHz)). However recent scientific literature has shown the potentialities of slotted approaches (among them MS-Aloha [5] seems to be the most extensively studied one).

The present paper analyzes what solutions can restrain the security-threats affecting vanets. These solutions are investigated together with their dependency on the underlying MAC protocol: as depicted in Fig. 2, the solutions are manifolds and not all of them are suitable for all MAC protocols.

1.1 Slotted Vanets – MS-Aloha

MS-Aloha is a slotted protocol which specifically addresses the issue of determinism in vehicular communications exploiting distributed contention methods. The wireless medium is managed in a slotted frame structure, with a fixed number of slots and fixed slot length. A global synchronization is required and is supposed

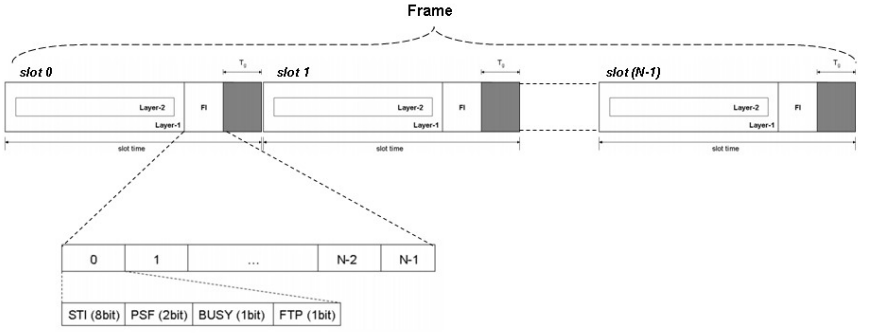

Fig. 1. Two-layer description of a MS-Aloha slot (PHY and MAC), including *FI* format

to be provided, for example, by a GPS/Galileo receiver. Concerning wireless physical layer, any one could be adopted and, to facilitate possible integration with IEEE 1609 stack, that of IEEE 802.11p is supposed to be adopted.

In MS-Aloha, before transmitting, each station has to sense the medium in order to identify unassigned slots and randomly select one of them. Collisions may still occur in this "contention" phase, especially in case of hidden stations. While WiFi foresees the well-known RTS/CTS handshake to overcome this issue, MS-Aloha uses message broadcasting: each "active" node continuously propagates its view of frame allocation in a fixed trailer called FI (Fig. 1). If the frame includes N slots, each FI contains $N \times FI_i$ fields, each 12-bit wide and specifying if the i-th slot is perceived free or busy, and to which node it is allocated (in its view)- a short node identifier is used for this purpose [5]. Each sub-field FI_i (Fig. 1) is made up by the following bits:

- **STI (*source temporary identifier*) - 8 bit:** the short label identifying the node heard on slot i.
- **PSF (*priority status field*) - 2 bit:** priority bits used for pre-emption mechanisms.
- **BUSY/CLS - 2 bit:** describing the slot i as free, busy, collision, or third hop (to limit the propagation of the FI information at third hop).

In practice, if a terminal M needs to transmit, it carries out a *contention phase*: it tries to gain access to a slot (chosen among those perceived "free"), after sensing the channel for a whole frame period. The node sends then a broadcast frame on the chosen slot (say slot j). All the nodes which have already been allocated a slot broadcast back their view of the frame, specifying if they have "heard" node M in slot j. This mechanism acknowledges node M of its transmission: if it receives just an FI containing contradicting information on slot j, it infers a collision and selects a new slot.

Each node refreshes the information on slot i when the frame has reached again the position i (the information on slot allocation expires after a frame-time). In order to improve slot re-use and make the protocol more deterministic [5], all the information on channel state which has not been directly detected by

a node – and comes only from the analysis of the received FIs – is not forwarded over more than one hop. This way the same slot is *not* announced "busy" too far from the node which is using it, improving slot reuse.

MS-Aloha has been defined and simulatively demonstrated to work under mobility with encouraging results.

2 Security Solutions and Vanet Protocols

Some solutions can be designed in a protocol independent way (as the layer-2 authentication solution proposed in sect. 2.1). Other well-known solutions have been designed for a specific protocol but can be easily extended to other ones: it is typical of the upper layers in the protocol stack. For instance IEEE 1609.2 (*Security Services for Applications and Management Messages*) [3] covers methods for securing WAVE management messages and application messages: despite what has been defined for IEEE 1609 [2] stack, they may also apply to slotted approaches, as in case of the Public-Key Infrastructure presented in 2.3.

Fig. 2. Cross-layer protocol-dependent and protocol independent mechanisms for vanet e-security

Finally there are mechanisms which apply only to a specific protocol class, as the one presented in sect.2.2 for slotted approaches: since such protocols include rich set of acknowledgements sent by each node, this gives the opportunity to enforce security (in terms of DoS prevention) by consistency checks.

Additionally, not only different services require proper security mechanisms, but also, reversely, each mechanism may suite particularly well a specific need. This perspective indeed is the one adopted in this paper, and the different available mechanisms are investigated in a bottom-up sequence.

The analysis leads to conclusions which can be summarized as follows: the only way to guarantee message and node authentication, as required by vanet safety mechanisms, is to exploit the PKI infrastructure (as widely published in literature); however also link layer encryption can play its role, mainly in segmenting broadcast domains without involving heavy protocol overheads; moreover some Denial-of-Service attacks can be counteracted only at MAC layer.

All in all, application layer security is the essential security tool but it is not the only required and not always affordable.

2.1 Link-Layer: Lightweight Security

The WiFi traditional authentication and encryption methods (such as WEP, WPA and WPA2) are often disregarded for vanets for several, sensible reasons. Among them the following ones: *(i)* they rely on a concept of centralized authentication by the infrastructure (AP) – which can hardly fit the ad-hoc paradigm – and the provided security suites more unicast than multicast and broadcast traffic; *(ii)* the overall authentication scheme relies on the sharing of a common key among a large number of nodes or, alternatively, it requires an EAP-like protocol which can hardly scale for all the nodes and face their mobility; *(iii)* the identification of the users is not guaranteed especially for broadcast transmissions; *(iv)* given the large number of cars participating in a vanet and sharing the secret access keys and the large number of road-infrastructures, the keys should have geographical and temporal terms.

In particular the third point has recently been appointed as the main weakness of the WiFi Protected Access [6] in the so called *Hole 196* vulnerability. Central to this vulnerability is the Group Temporal Key (GTK), shared among all authorized clients in a WPA2 network. Typically only an AP is supposed to transmit group-addressed data traffic (encrypted using the GTK), however, nothing in the standard stops a malicious authorized client from injecting spoofed GTK-encrypted packets. It means that an insider (authorized user) can sniff and decrypt data from other authorized users and inter-user data privacy among authorized users is inherently absent. For sake of clarity, the Advanced Encryption Standard (AES), on which WPA2 is based, has not been cracked by *Hole 196*.

So far the following scheme is proposed for link-layer baseline security:

- the encryption mechanism of WPA2 (derived from AES block cipher) is preserved;
- since vanet traffic is mainly broadcasted, encryption uses only GTK; consequently GTK must change often over time; for simplicity GTK *may* may be derived from a Group Master Key (GMK) as in 802.11 std, for instance enforced by *rotation* mechanisms;
- all the communications must be encrypted and the key is shared within a given area; as a result encryption is useful to insulate traffic among separate regions: for instance a highway and a contiguous urban street can define logically separate vanets and, correspondingly, separate broadcast domains are defined;
- the key(s) may obtained by authentication with central authority over a PKI infrastructure; in this case the process falls under the application-layer security umbrella and: *(i)* the infrastructure gains a more scalable control on the paths (without overhearing all the wireless traffic) and a more precise control with respect to the ingress-egress gates; *(ii)* the nodes collect transactions receipts which also certify their paths. Such certification could also be used for advanced traffic management schemes (for instance to award credits as prizes to *green routes*);
- the nodes are supposed to be provided with more keys (they could also be contemporaneously used for decryption), in order to manage temporal

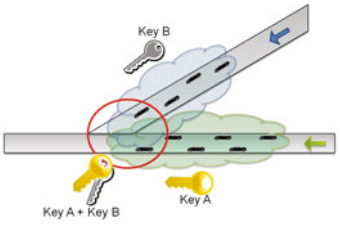

Fig. 3. Key management scenario: an intersection between areas where different keys are used. Vehicles in the red circle must know both Key A and Key B.

validity and spatial hand-off; the proposed scheme has several infrastructure checkpoints that manage key distribution in the different areas. This segmentation helps to split the broadcast domains in cases (i.e. highway near a city, or overpasses) where different logical areas are physically close to each other. However, a vehicle could happen to be in the transmission range of a confining area it is approaching to, in which a different key is used. Moreover, vanets are typically affected by fading [16] [17], which could make it difficult to define strict region boundaries. In order to avoid decoding problems and improve security, every mobile node is supposed to know and preserve also the keys used in the neighbor areas, and to be able to use all of them to decrypt the received messages (see Fig.3). The spatial validity of a key is supposed to be associated with a geographic area (e.g. city or region) that can be hypothesized to be wide and well defined;

- aspects such as message and node authentication and encryption of unicast traffic are left to upper layers; to say it more formally, in order to evaluate the messages received a node can build its own trust model about the sender, and the certification of the message has a predominant role in this;
- considering the limited scope of the encryption, the only issue concerns what happens if a malicious user is forwarded the GTK, skipping the authentication; notably its transmissions could not be prevented but it would be discouraged by the existing upper-layer security mechanisms.

In this way, this first level of security allows to segment a single vanet domain into smoothly separate areas; additionally the infrastructure achieves a first (not fully certified, but simplified) knowledge of the identity of the vehicles in the networked area. Finally, the proposed link-layer security does not constitute a true security solution but something worth when upper security layers are provided.

2.2 MAC Layer: DoS Prevention

Also Medium Access Control protocols can introduce weaknesses which can be exploited for Denial-of-Service (DoS) attacks - pure jamming approaches will not be considered because they destroy every kind of radio communication in the attacker's frequency band. This is, evidently, a MAC-protocol dependent issue: for this reason it will be analyzed separately for CSMA/CA and for MS-Aloha.

CSMA/CA implies that all the nodes are fair in computing collision-avoidance waiting time. If any station did not follow the CSMA/CA rules, it could *(i)* gain a higher bandwidth than it should (*unfairness*); *(ii)* prevent transmission by the other nodes (*pure DoS*). Unfortunately such behaviors could be hardly discovered in CSMA/CA, because hidden station cannot be excluded and each node has a thorough knowledge only of its own view of the channel: as a result it cannot infer possible violations to the CSMA/CA rules.

In MS-Aloha instead, the violations are more evident (unless pure jamming is considered) and, reversely, the attack can be twofold: a node can either attempt to access more slots than it can (*unfairness*) or cause logical collisions in order to block any transmissions (*pure DoS*).

Fortunately in MS-Aloha there is plenty of redundant information. For each slot, indeed, every node can receive up to N (number of slots per frame) state indications. In the typical configuration, every frame has 224 slots, resulting in a large number of information about the channel state. So, conceptually, it is possible to leverage on such redundant information to identify and manage nodes trying to disturb/disrupt the communication with fake information about the slot occupation.

More in practice, it is easy to understand how FIs with wrong slot indications can cause a complete blocking of the available resources. Also malfunctioning nodes can cause similar effects.

The initial hypothesis is that the channel state perceived by close nodes is almost identical. In an area of about 80 meters around the node (where the PDR -Packet Delivery Rate- is still about 90%), the involved nodes should see the same channel status. From this starting point, it is possible to infer possible inconsistent slot allocations. Depending on the way FIs are modified, two kinds of attack can be driven: 1 - the FIs sent are completely random, inconsistent with the other ones; 2 - the FIs are generated starting from a genuine one, changing only some fields. The more an FI is not coherent with the other ones, the easier the identification of suspicious behaviors is. Intuitively, if an attacker transmitted FI information only slightly counterfeited, it would be harder to identify it.

An example is shown in Fig.4: node D wants to unfairly gain control on the full channel. For this purpose it can mimic collisions by itself and by other nodes: thus it announces an FI containing the sequence D,J,M,E,F and then spooves such node identifiers (independently of their real existence): this way the full channel would be first freed and then maliciously engaged by D. However spatial and temporal correlation (of the received FI) can be exploited to prevent this by evaluating the dependability of the FI information received.

The simplest case is a node at one-hop distance which collects a certain number of coherent FIs before signaling a collision (thresholds should vary with the density of vehicles in the network). If a single node signals a collision in slot i, in the following frame the collision is validated only if other nodes confirm a direct sensing of the same collision, otherwise the FI is discarded as a fake. Additionally, correlation among FIs can take place also in the time domain.

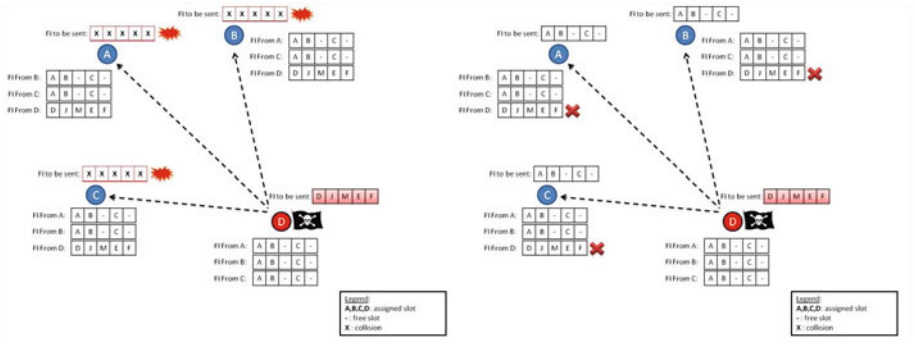

Fig. 4. Exploitation of correlation among FIs for the identification of misbehaving nodes: the case of Malicious Station with node D causing fake collisions

The logic can be further refined and summarized in the following way:

- each FI subfield can be evaluated separately;
- any FI information is "accepted" only if it is confirmed by a given number of nodes; this also prevents problems due to the sudden appearance of a node, as for a car exiting a garage: such node is supposed to accept the FI status of the other nodes (outside the garage) and not to disrupt the overall current slot assignment. Such approach would additionally increase MS-Aloha stability and robustness in general, it does not just prevent security threats;
- the mechanism of correlation is enriched with a weight for information, which takes into account what has been announced in the past from the same node and slot: for instance one approaching node can be inferred by FI and slot collisions validated 'straightforward' as soon as they take place (this recalls some concept derived from literature on reputation [10], [11]);
- each slot state transition (*e.g. free-busy, busy-collision, ...*) can be assigned a specific evaluation criterion. Here the novelty and the potential is high and is enabled once more by the redundant information available in MS-Aloha: the topic requires an analysis which can hardly fit the limit of this paper. However, just to make a practical example, the trasition busy-collision is mentioned again. If node C causes a collision on slot J, it is anyway expected to have been previously sensed by a set of nodes (at two-hop distance). Such nodes can enforce it, increasing the number of the nodes notifying the same transition. Similarly each transition could be differently enforced by the distributed intelligence of the vanet.

It is worth mentioning that, in principle, the FI classification should distinguish and differently manage the cases of malicious and malfunctioning nodes (which should be flagged but not banned).

Finally, for sake of completeness, at MAC layer, a recent advance should be mentioned: a side aspect of security is privacy and in [15] it has been demonstrated to be enforced by leveraging on the use of pseudonyms.

2.3 Application Layer: Vehicular Security by PKI

With the previously described methods it is not possible to authenticate the information from a given vehicle, but only to deal with DoS attacks or malfunctioning vehicles. Especially for critical information (e.g. ambulance, police) the security becomes mandatory and strict, therefore it is necessary to add more robust security levels, providing authentication, integrity and non-repudiation.

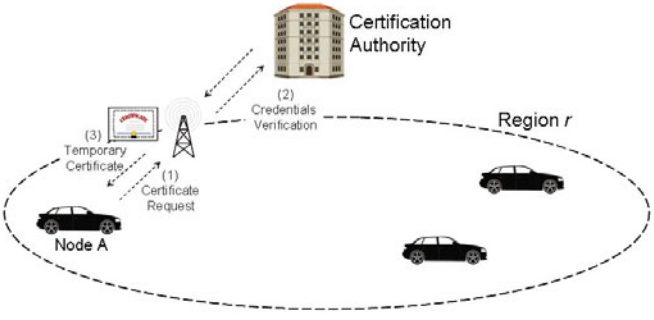

Fig. 5. PKI architecture applied to Vanet

The ideal architecture for such services is a public key infrastructure (PKI) with digital certificates. This approach presents some problems as it is introduced on mobile networks with high density [12]. Management of cryptographic keys and the CA hierarchy, control and revocation of certificates [13] are some of the open issues to be solved. Altogether they also set the issue of scalability: if all the messages were authenticated by the PKI infrastructure, each node should continuously - for each message - get, decrypt and check certificates, and check the appended hash. This can be hardly managed at wirespeed for all transmissions and cannot be either deferred (due to safety implications) or pre-computed (because the nodes are too many).

For this reason it is here proposed that this process is carried out only for critical information and entities (e.g. ambulance, police). This brings also some benefits in terms of protocol overheads, which are particularly relevant for slotted protocols, due to the fixed lengths and the already existing overheads. Considering the well known PKI [14], trailers are appended in the following way:

$$\mathrm{A} \longrightarrow \mathrm{B} : M \parallel \mathrm{E}_{KR_a}\left[\mathrm{H}(M)\right] \parallel \mathrm{E}_{KR_{as}}\left[T \parallel ID_A \parallel KU_a\right]; \tag{1}$$

A is sender, B the receiver, M the message, $\mathrm{H}(M)$ its hash and E_{KR_a} and $\mathrm{E}_{KR_{as}}$ respectively the private key of A and of the CA.

On one hand keys need to be short in order not to make the overhead too heavy; on the other hand, for the sake of driver's security, the shorter a key is, the shorter its life-cycles must be too. However a short life-cycle has its drawbacks: the PKI consists of several parts, and includes logical components (protocols) to manage the keys (distribution and revocation) – such protocols are exchanged

more frequently with shorter life-cycle and may impact on the delays and even affect available bandwidth.

Fortunately some quite recent approaches, such as Elliptic Curve Cryptography (ECC) [14], offer an excellent level of security with shorter session keys. For instance 160-bit ECC are comparable – in terms of robustness – to 1024-bit RSA/DSA, which offer a widely accepted level of security.

The hypothesis of ECC seems particularly reasonable for vanets at least for two reasons: longer packets are more likely to be discarded (due to higher number of errored bits which cannot be recovered by CRC); messages are required to be short for medium access efficiency in CSMA/CA. Concerning the latter aspect, it has however also beneficial effects on slotted approaches, such as MS-Aloha. In fact a 160-bit key would generate a node's certificate (the last part in chain (1)) which could be housed in the FI (which is supposed to be 224x12 bits). Reversely the message and its hash would be sent in the ordinary way (inside the payload). Consequently if it is accepted that the emergency messages substitute the FI with the node's certificate, a slotted approach may gain even more, in terms of efficiency, than it has been demonstrated so far [18].

2.4 Concluding Remarks

In summary, the paper has analyzed one of the most important aspects about vanets: the security of communications. For the IEEE 802.11p standard, a scheme based on CSMA/CA has been chosen, but some promising approaches, based on TDMA schemes, are emerging for MAC layer in vehicular networks. This paper has addressed the main topics, open issues and possible solutions for securing both asynchronous and slotted vanets.

Notably the analysis reveals that slotted approaches (MS-Aloha in particular) can exploit the redundant information carried by the protocol itself. This feature allows to implement security mechanisms on top of the original MAC protocol, without requiring substantial modifications. In particular, the proposed mechanism is based on a lightweight authentication of messages by means of correlation of the information broadcasted from every node. Conversely, such benefits do not hold for CSMA/CA.

Additionally MS-Aloha and CSMA/CA can both support the same security mechanisms at lower and upper layers, respectively with link-layer encryption and a proper adaptation of the PKI architecture.

In conclusion vanets are well setup in terms of security tools and slotted solution may offer some additional perspectives.

References

1. IEEE 802.11p TG. IEEE 802.11p/D9.0, Draft Amendment for Wireless Access in Vehicular Environments (WAVE) (September 2009)
2. IEEE 1609 WAVE Standards, `vii.path.berkeley.edu/1609_wave/`
3. IEEE 1609.2 Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, `vii.path.berkeley.edu/1609_wave/`

4. Shakkottai, S., Rappaport, T.S., Karlsson, P.C.: Cross-layer design for wireless networks. IEEE Commun. Mag. 41(10) (October 2003)
5. Scopigno, R., Cozzetti, H.A.: Mobile Slotted Aloha for Vanets. In: IEEE VTC Fall, pp. 1–5 (September 2009)
6. Ahmad, S.: Hole 196, Black Hat (2010), http://www.blackhat.com/html/bh-us-10/bh-us-10-home.html
7. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., Hubaux, J.-P.: Secure Vehicular Communication Systems: Design and Architecture. IEEE Communications Magazine, 100–109 (November 2008)
8. Aslam, B., Zou, C.: Distributed Certificate and Application Architecture for Vanets. In: MILCOM, pp. 1–7 (October 2009)
9. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, 38–47 (February 2004)
10. Despotovic, Z., Aberer, K.: P2P reputation management: Probabilistic estimation vs. social networks. The International Journal of Computer and Telecommunications Networking, 485–500 (March 2006)
11. Mui, L., Mohtashemi, M., Halberstadt, A.: A Computational Model of Trust and Reputation. In: Proceedings of the 35th Hawaii International Conference on System Science, HICSS (2002)
12. Raya, M., Hubaux, J.-P.: The Security of Vehicular Ad Hoc Networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 11–21 (2005)
13. Raya, M., Papadimitratos, P., Hubaux, J.-P.: Securing Vehicular Communications. IEEE Wireless Communications Magazine (October 2006)
14. Stallings, W.: Cryptography and Network Security, 3rd edn. Prentice Hall, Englewood Cliffs (2003)
15. Schaub, F., Kargl, F., Ma, Z., Weber, M.: V-tokens for Conditional Pseudonymity in VANETs. In: Scopigno, R., Cozzetti, H.A. (eds.) Proceedings of IEEE Wireless Communications and Networking Conference, WCNC 2010 (April 2010)
16. Nakagami, M.: The m-Distribution, a general formula of intensity of rapid fading. In: Statistical Methods in Radio Wave Propagation: Proc. Symposium at the University of California. Permagon Press, Oxford (1960)
17. Sklar, B.: Rayleigh Fading Channels in Mobile Digital Communication Systems Part I: Characterization. IEEE Communication Magazine, 90–100 (July 1997)
18. Scopigno, R., Cozzetti, H.A.: Evaluation of Time-Space Efficiency in CSMA/CA and Slotted Vanets. In: IEEE 71th Vehicular Technology Conference, VTC Fall (October 2010)