Towards Effective Security Framework for Vehicular Ad-Hoc Networks

Bartosz Lipiński, Wojciech Mazurczyk, Krzysztof Szczypiorski, and Piotr Śmietanka

***Abstract*—Vehicular Ad-Hoc networks (VANETs) have been identified as a key ICT technology for significantly improving, among others, road safety and transport efficiency. However, recently many security issues have been identified which require immediate attention and effective solutions. This paper is a first step towards providing a comprehensive security framework for VANETs. It includes mechanisms for exchanging messages in a secured manner. Additionally, it provides means to monitor and to secure routing protocols, as well as to detect and remove untrusted nodes from the network..**

***Index Terms*—VANET, security framework, authentication.**

I. Introduction

Vehicular Ad-Hoc networks (VANETs) have been envisioned as one of the most promising ICT technologies that could be utilized for many purposes, such as road safety, route planning assistance, tolling, traffic management, etc. However, in the real-life implementations, it is crucial to secure all the actions performed in the vehicle network from the potential malicious activities. However, due to wireless character, dynamic topology and difficulties in providing constant connection to the central element, securing VANETs is not a trivial task and thus it still requires a great deal of research and much effort from the scientific community.

Therefore, the purpose and the contribution of this paper is to make a first step towards secure VANETs by introducing a comprehensive security framework which includes mechanisms for exchanging messages in a secure and authenticated way. Additionally, the framework provides means to monitor and to secure routing protocols, as well as to detect and remove untrusted nodes from the network.

The rest of this paper is organized as follows. Related work is presented in Section II. Next, requirements for VANETs security mechanisms are presented in Section III. In Section IV possible attacks on VANETs are discussed, including attacks on Ad-Hoc routing protocols. In the next section detailed description of proposed security framework is presented. A summary in Section VI concludes the paper.

II. Related Work

In the existing literature, many proposals of security architecture for VANETS can be found. Below we list the most important ones.

In [1], Kamat *et al*., propose an identification-based architecture for securing VANET. However, to meet privacy requirements, each vehicle must obtain a pseudonym from RSU. Such solution requires an existence of master secret (pseudonyms creation algorithm) in each RSU, which jeopardize security of the whole architecture.

Security architecture based on trusted groups has been proposed in [2], by Wagan *et al*. Authors suggest creation of a group of vehicles and election of its leader. Elected node would be responsible for generation and distribution of transmission keys to group members. Unfortunately, those processes can be very ineffective due to the frequent changes in mutual positions of nearby vehicles in typical road traffic scenarios, and can result in high bandwidth utilization.

Chaurasia *et al*., in [3], propose solution for nodes authentication performed by RSU. Drawback of such approach is the necessity of providing the full RSU range coverage for considered area.

In [4] Zhu *et al*., presents architecture similar to [3]. Author increased the role of RSU by involving them into aliases granting process and in assistance in exchange of symmetric transmissions keys for each pair of vehicles.

The main difference between mentioned architectures and the framework proposed in this paper is the scope of addressed security requirements and number of considered security issues. Existing architectures ensure only basic requirements for securing communication between VANET nodes (i.e.: authentication, confidentially and data integrity). Furthermore, presented architecture, unlike those mentioned before, strongly connects trust management of a particular node with the network management to provide reliable communication. In authors' opinion, main drawback of existing security architectures is that RSU have a crucial role in providing network services, which implicates very high deployment costs. In presented architecture, due to the limitation of RSU role in communication, and nodes' ability to store a number of certificates, initial deployment requirements have been reduced.

III. Security Requirements for Vehicular Ad-Hoc Networks

In this section we list requirements, which must be fulfilled by a security framework for vehicular Ad-Hoc networks [5].

A. Authentication

Every message received by a VANET node must be

Manuscript received August 27, 2014; revised March 12, 2015. This work has been founded by MOBITRAFF Project (INTER-PolLux programme) financed by NCBR (Poland) and FNR (Luxembourg) agencies.

The authors are with the Warsaw University of Technology, Institute of Telecommunications, Poland (e-mail: blipinsk@mion.elka.pw.edu.pl, wmazurczyk@tele.pw.edu.pl, ksz@tele.pw.edu.pl, psmietan@mion.tele.pw.edu.pl).

DOI: 10.7763/JACN.2015.V3.155

authenticated, to confirm that the sender is really a node which it presents itself to be.

B. Availability

A network should be able to operate, even under attack or other unexpected circumstances. For the purpose of high availability, redundant methods of communication should be designed, in case of the occurrence of an unusual behavior in the network.

C. Data Integrity

Each node in the network must be able to verify if messages exchanged between the sender and the receiver were not tampered during transmission.

D. Privacy

Implemented security mechanisms cannot cause nodes' privacy loss. Therefore, the main aim is to avert the ability of vehicle/driver tracing or capturing his sensitive data. That is why it is vital to obfuscate the correlation of the message with its sender, so that the other receivers cannot unambiguously find out the source node.

The ability of unambiguously uncover the identity of the node should only be granted to the authorized organizations.

E. Small Overhead and Support for Real Time Applications

Due to the limited transmission resources, both in available bandwidth and duration of communication sessions, algorithms and protocols used to secure the network should consume as little bandwidth as possible, and perform their tasks without unnecessary delay.

F. Data Verification

Network should have mechanisms to perform verification of usable data for their conformance with reality. Furthermore, algorithms for faulty nodes detection and removal from the network should be provided.

G. Protection of Routing Protocols

Transmissions over longer distances are provided using intermediary nodes. This means also involvement of all nodes e.g. in the routing information exchange. The lack of proper mechanisms to ensure routing protocols security enables attacker to delay or interrupt proper communication.

H. Non-Repudiation

Nodes involved in the messages exchange cannot deny their participation in communication session. This feature could be very important for VANETs, e.g. in case of a traffic accident, when the reconstruction of events and participants is crucial for determining its causes.

IV. Attacks in VANETs

There are a number of potential attacks that can be performed in VANETs. The main motivations for these attacks are:

1) To disrupt the use of the network for ordinary users.
2) To propagate false information about events on the road.
3) To steal confidential information (e.g. using phishing techniques).

VANETs are prone to the well-known types of attacks such as Denial of Service (DoS), eavesdropping and data modification (Man in the Middle - MitM), nodes identity spoofing, or timing attacks (attacks using time delays).

However, the most dangerous types of attacks for VANETs, in our opinion, are those listed and described below. Each of presented attacks is a consequence of violation in security requirements described in previous section. Methods used for detecting and preventing these attacks are addressed by the proposed security framework. The only exception is a GPS spoofing attack, whose countermeasure is described in this section, as GPS is not considered as a core part of VANET.

A. Denial of Service (DoS) and Distributed Denial of Service Attacks (DDoS)

Violated security requirement: *availability*.

The basic concept of DoS attack is based on deliberately preventing network communication from succeeding. Defending against this type of attacks is especially difficult to implement due to the various ways that it can be accomplished with. To perform DoS attacks in vehicular Ad-Hoc networks two major techniques are utilized:

1) Disrupting the frequencies which are being used for wireless communication. In this method attacker must place the transmitting device in a given frequency range and begin sending a random signal. This would make the communication between the nearby nodes practically impossible. The effectiveness of the attack depends mainly on the transmitting power of the jamming device.
2) Sending large amounts of network data by an authorized host. Generated network messages are valid network frames (in contrast to random signal from previous technique mentioned above), but the huge number of them disturbs network operation causing serious congestion and in result inability to communicate between the legitimate nodes.

Each of the above mentioned types of attack can be performed simultaneously by a group of malicious nodes. Such attack is called DDoS. Distributed attack with proper nodes allocation can be much more dangerous than typical DoS. Limitations of DoS are mostly caused by the limited transmission range of a single node.

B. Sybil Attacks

Violated security requirement: *authentication*.

Sybil attacks in VANETs are based on spoofing a single network node's identity by many bogus vehicles (non-existent in reality) and flooding the network with incorrect information. Network node performing the attack (the attacker) sends multiple copies of the same message (containing false data), using unique counterfeit identities in each generated message. In result, a lot of messages from different senders containing the same data are being circulated in the network. This attack can become a serious threat when a single node is able to force other vehicles into acceptance of the false messages and to treat them as legitimate ones.

C. Sending Bogus Information

Violated security requirements: data integrity, data

verification.

This type of attack relies on deliberate injection of false information into the network by one of the nodes to create a virtual representation of a specific situation on the road. In most cases an attacker wants to create a certain kind of chaos in the network, resulting in a specific reaction of other nodes. For example, node sending false information may inform others in the network about (non-existent) traffic jam, accident, or closed road, suggesting other drivers to choose other way.

There are three approaches to perform such attack by:

1) Creating or modifying network frames

Malicious node injects newly created frames to the network or modifies existing frames with fabricated content.

2) Repeating captured network frames (replay attack)

The attack relies on capturing of the communication (the raw frames) in the VANET and injecting it into the network later. A notable example of using this attack is to repeat packets sent by ambulance to obtain a faster ride.

3) Misleading vehicle sensor (illusion attack)

The difference between previous approaches is that Illusion attack is not based on injecting false information to the network, by creating new or changing existing network frames. The idea relies on tricking car sensors, which may lead to the generation of the specific messages and sending them into the network (e.g. information that the car has been involved in an accident, bad weather conditions etc.).

D. Man in the Middle (MitM) Attacks

Violated security requirements: *data integrity, privacy.*

These attacks rely on eavesdropping and modification of the network traffic. There are no significant differences between Man in the Middle attacks in VANETs and MitM attacks in typical wired networks. This attack affects negatively the authenticity of transmitted information, and may significantly compromise network security.

E. Wormhole Attacks

Violated security requirements: *data verification, protection of routing protocols.*

Wormhole attack is based on receiving frames from one part of the network and injecting them into another part of the network. It is known to be one of the most dangerous attacks in Ad-Hoc networks. In order to be effective a tunnel between two attacker hosts is required (using any transmission technique available). After it is established, one host collects information and sends it to the end of the tunnel, where it is injected into the different part of the VANET network. Wormhole attack can be especially dangerous for the typical routing algorithms such as AODV (Ad-Hoc on demand) and DSR (dynamic source routing).

F. GPS Spoofing

Violated security requirement: *data verification.*

This attack is not a direct attack on VANET network. However, due to the fact that the knowledge of the position and time is used, it is considered in security analysis for VANETs. GPS spoofing is based on sending better and stronger GPS signal by an attacker, which results in fake vehicle position or time. This attack could also use signal recorded earlier to provide nodes with a different time (replay attack) or a different location (wormhole attack).

Currently protection methods against such attacks have been proposed [6] and they rely mainly on monitoring and correlation of power (as well as other parameters) of received signals.

G. Routing Protocols Attacks

Violated security requirements: *protection of routing protocols, non-repudiation.*

Despite the fact that most of the traffic in the VANETs is purely broadcast, there might be a need for communication between two specific nodes, not staying in their mutual radio coverage. To allow such kind of transmission using intermediate nodes, classic routing protocols for mobile Ad-Hoc networks, are being utilized. Unfortunately no security solutions against possible attacks have been embedded in those protocols [7].

Generally, attacks on routing protocols can be divided into two groups: active and passive attacks.

1) Active attacks: attacking node deliberately injects bogus routing information into the network, which prevents or hinders the operation of the routing protocol (in a certain part of the VANET). Such actions may lead to [8], [9]:
   - Extension of packet route;
   - Creation of routing loops;
   - Redirection of the traffic to a non-existent node (i.e. blackhole attacks);
   - Redirection of the traffic to attacker's node (i.e greyhole attacks) in order to drop it, temporary store it, or modify it (i.e. Man in the Middle attack).
2) Passive attacks: attacking node does not interrupt normal operation of routing protocols, but tries to gather some valuable information through analysis of routing updates. This kind of attack can lead to the discovery of information such as: network topology, location of the nodes or their role in the network.

V. Security Framework Proposal

In the following section the detailed description of the proposed VANET security framework will be presented. The main idea of the framework is also illustrated in Fig. 1.

A. Assumptions

Proposed security framework is based on the following assumptions:

1) Each node is equipped with GPS receiver,
2) One, central point for the whole system exists that later will be referred as VSIC (VANET Security Information Centre),
3) Each node has sufficient memory capacity for storing certificates and CRLs (Certificate Revocation List – containing certificates that have been revoked from the network, by the certification authority),
4) Road Side Units (stationary VANET nodes, usually managed by a public institution): (i) do not have to provide full coverage of roads; (ii) are equipped with at least two antennas; (iii) have a constant communication with central point of the system (VSIC).

B. Framework Basics

The primary mechanism for the whole framework is based on the usage of public key infrastructure (PKI). In this approach each network node has its own inseparable pair of keys (a public key and a private key). It is a typical example of implementation of an asymmetric cryptography. A car wishing to send a message encrypts it using public key of a receiving vehicle. The receiver (message destination node) has to use its own private key to decrypt the incoming data. As the name itself states, public keys are not secret. They are known to all the nodes that want to communicate with the owners of the corresponding private keys (which are being known only to their possessors). Such communication scenario (node to node with encryption) will be mainly utilized for messages exchange between vehicles and the RSU, and further to the VSIC. However, majority of the messages in VANETs are send as a broadcast, so transmitting node does not perform any key exchange with listeners. Sender can encrypt message with his private key, however, in our opinion, encryption for broadcast transmission is not mandatory.

For the purpose of node authentication, public key infrastructure enforces the introduction of additional institution, called authorization center, which role would be to distribute key sets (pairs). Every node willing to acquire its own set of keys has to go through identity verification procedure handled by previously mentioned trusted site. After that, the part of the institution called certificate authority (CA) would be eligible to verify the identity of the node during message transmission. For VANETs this trusted site could be e.g. The Ministry of Transportation. The verification process is possible thanks to certificate created by the CA exclusively for previously verified vehicle. The issued certificate will be used to authenticate exchanged messages.

C. PKI Privacy-Related Risks

If a single node is using the same public key for a relatively long time, it can become easily traceable. To prevent this threat, trusted site (authorization center) will have to grant a whole set of key pairs so that the vehicle could use them interchangeably [10]. Additionally, frequency of key rotations will be associated with the density of vehicles around. Adopting such technique makes it more difficult for the attacker to find a correlation between the keys and the vehicle. The maximum frequency of changes should also be regulated to avoid situations which could be treated as a Sybil attack.

D. Key Distribution

Undoubtedly, the way of handling new keys distribution, updating current ones and withdrawing cancelled could be problematic. The perfect solution would be if every single node had the ability to connect to authorization center at any time, to update the key-set relevant information. Even if cellular networks are used for this purpose we cannot assume, that the node is able to reach the CA at any time. Hence, presented framework does not assume constant connection. Updates of certificates will be performed whenever vehicle is in the range of RSU. Cellular network could be used as a backup, but connection through RSU is preferred. Each vehicle should be capable to store a pool of certificates, to allow VANET operations in periods between the updates.

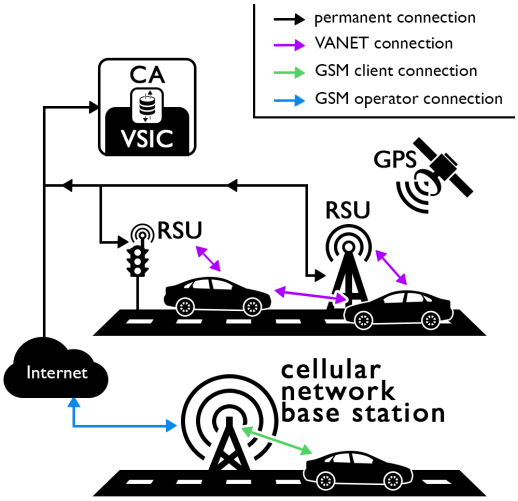

Fig. 1. Proposed framework scheme.

E. Certificates Characteristics

Every network node would be granted two different types of certificates. The first type, called: network-certificates, would be utilized for the basic communication in the network. Those certificates would be relatively short-lived to assure the frequent changes of certificates in the network (to provide privacy to vehicles). They can be provided by CA through communication with RSU (see the key distribution procedures section). The second type of certificates, CA-certificate, would be granted only, directly by the CA. The first set would be assigned immediately after the registration procedure. This type of keys would be used only to communicate with RSU for the purpose of communicating with CA (e.g. to request a pool of network-certificates). The expiration date of this type of certificate would be distant. Its expiration would be unambiguously related to the need of renewal of CA contract.

F. Content of the Secure Messages in VANET

To fulfill security requirements, each message sent within VANET will contain: a message *(encrypted or not),* certificate of the sender, hash of the message, timestamp.

A certificate will be used to check if the sender is a valid user of the VANET (in node-to-node transmission, certificate is included only in the first message). After receiving the message, node will check if sender's certificate is present on the CRL (method for gathering the CRL is described later in this section). If match is found, which means that the node has been removed from the network, the received message is dropped. Hash is used to verify data integrity. Timestamp is not used directly in the process of message verification, but is necessary to detect abnormal activities and protect against several types of attacks. With the timestamps comparison it is possible to detect wormhole attack [11] and replay attack [12]. Utilizing timestamps require synchronization of all clocks in the network, which can be accomplished using GPS.

G. Mutual Check

In wireless environment, many malicious activities can be noticed by neighboring nodes. In the proposed framework, each node is obliged to passively listen, analyze and verify all messages it receives, even if the node is not an active participant of the communication. Many VANET attacks,

especially attacks on routing protocols, could be detected in this way.

1) Monitoring communication in low layers of the network

Every node will monitor behavior of other nodes in the low layers of the network, i.e.: whether packets are not sent too frequently, if size of the packet is correct or whether the transmission power is not too high. Each of these activities could result in decreased network performance. Furthermore, as described in previous section, passive attacks on routing protocols can be detected by the sender, through checking whether next-hop node retransmits the message [13]. However, if an attack is performed by two or more colluding nodes in proper configuration, this method would fail. If nodes, which are not the part of the routing message path, also monitored the message retransmission, it is more likely to detect nodes acting as gray or black holes.

Furthermore, road side units will also participate in mentioned process. Thanks to their stationary character and multiple antennas, they are able to detect Sybil attacks [14], [15]. RSU can calculate the angle between passing car, and the position of the Road Side Unit. If a single network node tries to simulate the existence of many vehicles, the signals from each of these false nodes will be received by the RSU with the same angle (although they should be different). Moreover, measurements of the signal strength can be used to improve accuracy of detection [16].

2) Monitoring content of the messages

Each node will be also responsible for analyzing the useable content of every received message; even if the message is potentially not in his scope of interest (i.e. cars will analyze messages destined for trucks). Next, node can assign a level of trust for each message, which can be calculated based on: predefined set of rules, comparison with the messages received from other vehicles, information from VSIC and the data from vehicle sensors [17]. When the trust level exceeds predefined threshold, VANET equipment can ask the driver (e.g. by using display of on board computer) to confirm or deny particular situation, which was retrieved from VANET, or simply drop the message. If the driver contradicts the received information, a message with request for decrease of sender trust level will be sent to the VSIC [18].

H. Trust Management

Any vehicle that has detected a suspicious action of another vehicle is obligated to inform about it other VANET nodes. As it has been stated before, to maintain the privacy of the nodes, multiple certificates are being granted for every registered vehicle. The vehicle can use them interchangeably (as long as they are not outdated). Because of this reason, informing the network of suspicious behavior of a single node cannot be successful without an external entity. It is because specific node (at a specific time) knows only about the current certificates of the neighboring nodes. Therefore, from the perspective of a single vehicle, the potentially malicious node (the one for which the suspicious behavior has been spotted) after some time (e.g. after it had changed the certificate) may be identified as a normal node, that has not been reported to perform suspicious actions.

The proposed external entity as mentioned before is called VANET Security Information Centre. The VSIC database stores records for every single vehicle eligible to communicate through VANET (previously registered). Every record stores basic information about the vehicle (i.e. Vehicle Identification Number – VIN, Vehicle Registration Number, and others), information about certificates granted for this vehicle, and the corresponding, current trust level(s). If a specific vehicle is not able to communicate with the VSIC, it should create a message in the same manner it would when sending one to network (saving the creation time as the timestamp of the message), and queue it until it has the ability to communicate with VSIC.

The communication between network nodes and VSIC is significantly limited. Vehicles can only request for the current trust level of a particular vehicle that is currently using a specific certificate (and receive the reply), or they can request for a decrease of specific vehicle's trust level. The reason for such a significant limitation is the fact that VSIC stores much data that needs to be kept secret not to jeopardize the privacy of nodes. The latter mentioned request is the information that is being sent to VSIC after the suspicious action performed by a specific vehicle has been noticed. It's important to remember that any vehicle is eligible to send only a single Trust Decrease Request (TDR) about a single certificate. VSIC checks whether the limit has been reached. This constraint has been introduced to make it impossible for a single node to reduce significantly the trust level of another node.

The convenient way of implementing the VSIC would be to merge it with the CA. VANET Security Information Centre needs to hold identical certificates data as CA, so if those two entities had been implemented separately, they would have to synchronize their databases. The certificates distribution could be handled easily through the VSIC communication channel and the joint implementation would also positively affect the CRL distribution process.

Due to different attack targets in VANETs, two different types of trust levels are introduced: *environment data* and *routing data trust level*. The first one corresponds to the trustworthiness of any data being sent through VANET that represents the information about the environment of the vehicle. In other words: how much can vehicles trust any data that originates from the particular vehicle and states about e.g. situations on roads. The latter trust level represents the trustworthiness of the information being exchanged during operation of the routing protocols. This trust level can be converted to the routing protocol metrics. It is also possible to introduce other trust levels for more sophisticated purposes.

Any trust level should be implemented in a way that considers the robustness of the VANET and the discontinuous nature of communication with the VSIC. Due to the fact that messages generated by vehicles could be created earlier (and queued), are not related to the exact moment in which they have been received. The timeline for received Trust Decrease Requests should be recreated and analyzed in order to make a decision about potential decrease in a specific trust level.

The following paragraph describes the proposed implementation of the trust level. It is worth noting that it is exemplary and the implementation for real-life system should be designed specifically to effectively support the operation

of the whole VSIC.

Trust level could be considered as an integer value of a finite set – the higher the value, the higher the node's trust. For the purpose of this example, it is assumed that the trust level could reach the values from 0 to 3 (inclusive). Every node (normal – not malicious), would be granted almost the highest value by default (value 2). Nodes by default would be considered not-malicious (presumption of innocence). The highest level of trust (3) would be reserved for network devices only (that should always be trusted). The default value for nodes would remain as long as they do not present suspicious behavior. To prevent lowering the trust for vehicles that their normal behavior had been mistakenly taken for potentially malicious, the decrease of trust level can only happen if such behavior repeats frequently.

Fig. 2 presents an exemplary trust level calculation algorithm, repeated every *Trust Level calculation interval*. It would be performed inside VSIC to calculate current Trust Levels of vehicles. Trust level decrease is related to a specific number of TDRs (*decreaseTdrNum*) received in a specific period of time (*decreaseTdrTime*). For example: 10 TDRs per minute could result in decreasing the level by 1. Assuming the innocence of nodes, the corresponding limit should be introduced that would enable the increase of the trust level of network node (less than *increaseTdrNum* TDRs received in *increaseTdrTime*). This limit is proposed to be higher (harder achievable – e.g. less than 2 TDRs per 5 minutes). In other words, network nodes would be presumed to be innocent, but could easily lost network's trust, and could, but in a much more difficult manner, regain it.

Algorithm 1 Trust Level Calculation

```
1:  vehicle ← currently analyzed vehicle
2:  maxTrustLevel ← maximal Trust Level available for analyzed vehicle
3:  minTrustLevel ← minimal Trust Level available for analyzed vehicle
4:  decreaseTdrNum ← number of TDR required to decrease the Trust Level
5:  increaseTdrNum ← number of TDR required to increase the Trust Level
6:  decreaseTdrTime ← Trust Level decrease analysis window
7:  increaseTdrTime ← Trust Level increase analysis window
8:  mainloop:
9:  while true do
10:     if Is there any vehicle without updated Trust Level then
11:         vehicle ← vehicle without updated Trust Level
12:         if vehicle.tdrsInLast(decreaseTdrTime) > decreaseTdrNum then
13:             if vehicle.trustLevel() == minTrustLevel then
14:                 add all vehicle's certificates to CRL
15:             else
16:                 vehicle.decreaseTrustLevel()
17:             goto mainloop.
18:         else if vehicle.tdrsInLast(increaseTdrTime)<increaseTdrNum then
19:             if vehicle.trustLevel() != maxTrustLevel then
20:                 vehicle.increaseTrustLevel()
21:             goto mainloop.
22:     else
23:         wait Trust Level calculation interval.
24:         goto mainloop.
```

Fig. 2. An exemplary trust level calculation algorithm.

Table I presents an exemplary results of the proposed algorithm. It represents 10 steps of algorithm calculations (10 minutes) for a single vehicle. Second row of the table represents a number of trust level decrease requests received by VSIC for a particular vehicle in a specified minute. The third row consists of calculated trust level values for this vehicle at the end of each minute. The important thing to notice is that when calculating trust level for a specific column, the 'last minutes' phrase from the algorithm are inclusive with this specified column. In other words: when e.g. calculating trust level for column representing 6th minute ('6' in the first row), 'last 5 minutes' from algorithm represent columns with: 2, 3, 4, 5, 6 in the first row (total of 19 received TDRs). The default value of trust level for this vehicle is 2.

Presented example shows the difference in the way the algorithm allows for rapid loss of trust level, but is slow in its regaining. Vehicle lost 1 point in trust level when it received 12 TDRs in 3rd minute, but regaining it was a process that lasted from 4th minute till 8th. Two minutes (9th and 10th) with significantly raised number of received TDRs caused the trust level to be lowered to 0 and in result the vehicle to be expelled from any communication in the network.

TABLE I: EXAMPLE OF TRUST LEVEL CALCULATION

Time [minute]	1	2	3	4	5	6	7	8	9	10
TDR received during a single time interval	0	6	12	0	1	0	0	0	14	12
Calculated Trust Level for this vehicle	2	2	1	1	1	1	1	2	1	0

I. CRL Distribution

When a node reaches the lowest level of trust it should be expelled from the network. This action can be performed by adding all its current not-outdated certificates to so called Certificate Revocation List (CRL), and not granting any new certificates to this vehicle. This procedure can also be done manually by CA employees, e.g. due to the change in ownership of the car. Any other vehicle could send a request to VSIC for a current CRL (through a RSU), and not communicate with any vehicle that is using the revoked certificate. To optimize CRL obtaining process, revision numbers could be introduced and thus, only changes introduced since last update would be transmitted to requesting node.

VI. CONCLUSIONS AND FUTURE WORK

In this paper a comprehensive security framework for VANETs has been proposed, which resolves and/or alleviates majority of the mentioned threats and fulfils stated security requirements. The framework is based on a concept of Public Key Infrastructure with centralized CA, and utilizes RSUs as a relays in keys obtaining process. It also introduces trust management system with methods for storing (VSIC) and changing (TDR) trust levels for each node, and further distribution of CRL lists. Auxiliary methods for monitoring the behavior of the network nodes (in low network layers as well as in content of the messages) by each node and RSUs are also described. Future work will be to conduct detailed performance evaluation of the proposed framework. Additionally, simulation of framework software implementation can be also done together with road traffic simulators (e.g. SUMO - Simulation of Urban Mobility [19]), to test the framework's efficiency using real-life road scenarios. Moreover, future work should include verification of the level of delays introduced by the proposed framework

as they should not be excessively high to not to disturb VANET real-time applications such as transit signal priority (TSP).

It is also worth considering further improvements to implementation of the dynamic mechanisms of the presented Trust Level algorithm. This includes e.g. adjusting number of the required, received TDR to increase or decrease Trust Level for a given vehicle, based on the density of vehicles in the particular area.

REFERENCES

[1] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in *Proc. the Third International Workshop on Vehicular Ad Hoc Networks*, September 29, 2006.

[2] A. A. Wagan, B. M. Mugha, and H. Hasbullah, "VANET security framework for trusted grouping using TPM hardware," in *Proc. Second International Conference on Communication Software and Networks*, 2010.

[3] B. K. Chaurasia and S. Verma, "Infrastructure based authentication in VANETs," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 6, no. 2, April 2011.

[4] L. Zhu, C. Chen, X. Wang, and A. O. Lim, "SMSS: Symmetric-masquerade security scheme for VANETs," presented at the Tenth International Symposium on Autonomous Decentralized Systems, 2011.

[5] R. Kroh, A. Kung, and F. Kargl, "VANETS security requirements final version," *Secure Vehicle Communication*, 2006.

[6] H. Q. Wen, P. Y.-R. Huang, J. Dyer, and A. A. J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation*, 2005.

[7] T. Chen, O. Mehani, and R. Boreli, "Trusted routing for VANET," in *Proc. the 9th International Conference on ITS Telecommunications*, 2009.

[8] S. Biswas, J. Misic, and V. Misic, "Performance analysis of black hole attack in Vanet," in *Proc. the 31st International Conference on Distributed Computing Systems Workshops*, 2011.

[9] L. Chen, H. Tang, and J. Wang, "Analysis of VANET seciurity based on routing protocol information," in *Proc. the Fourth International Conference on Intelligent Control and Information Processing*, 2013.

[10] M. Raya and J.-P. Hubaux, "The security of vehicular Ad-Hoc networks," in *Proc. the 3rd ACM Workshop on Security of Ad-Hoc and Sensor Networks*, 2005.

[11] Yih-Chun Hu, Adrian Perrig and Adrian Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," in *Proc. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, 2003, vol. 3.

[12] G. Wittenburg, "A defense against replay attacks on Chaumian Mixes," Bachelor thesis, University of Berlin, 2003.

[13] M. Erritali and B. El-Ouahidi, "A survey on VANET intrusion detection systems," in *Proc. the 2013 International Conference on Systems, Control, Signal Processing and Informatics*, 2013.

[14] J. Grover, M. S. Gaur, and V. Laxmi, "A novel defense mechanism against sybil attacks in VANET," in *Proc. the 3rd International Conference on Security of Information and Networks*, 2010, pp. 249-255.

[15] G. Guette and B. Ducourthial, "On the Sybil attack detection in VANET," *in Proc. the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, 2007, pp. 1-6.

[16] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETS," in *Proc. the* 2006 *workshop on Dependability Issues in Wireless Ad-Hoc Networks and Sensor Networks*, 2006.

[17] N.-W. Lo and H.-C. Tsai, "Illusion ATTACK on VANET applications — A message plausibility problem," in *Proc. the IEEE Globecom Workshop*s, 2007.

[18] I. T. A. Halim, H. M. A. Fahmy, A. M. B. El-Din, and M. H. El-Shafey, "Agent-based trusted on-demand routing protocol for mobile Ad-Hoc networks," in *Proc. the 6th International Conference on Wireless Communications Networking and Mobile Computing*, 2010, pp. 467-483.

[19] SUMO simulator — Simulation of urban mobility. [Online]. Available: http://sumo-sim.org/

Bartosz Lipiński received the B.Sc. degree in telecommunications from Warsaw University of Technology, Poland, in 2013. His main research interests include steganography, information hiding techniques and wireless networks. He is a co-author of 3 publications.

Wojciech Mazurczyk holds a B.Sc., M.Sc., Ph.D. (honors) degrees and a D.Sc. degree all in telecommunications from Warsaw University of Technology, Poland, in 2003, 2009, 2004, and 2014, respectively. Currently he is an associate professor of Warsaw University of Technology. He is the author of more than 80 scientific papers, 1 patent application, and more than 30 invited talks on information security and telecommunications. His main research interests include information hiding techniques, network anomalies detection, digital forensics, network security and multimedia services. From 2013 he is an associate technical editor for the IEEE Communications Magazine.

Krzysztof Szczypiorski holds the M.Sc. (with honors), Ph.D. (with honors) and D.Sc. (habilitation) degrees in telecommunications from the Faculty of Electronics and Information Technology, Warsaw University of Technology, in 1997, 2007, and 2012, respectively. He is an associate professor at WUT. He also is the research leader of Network Security Group at WUT (secgroup.pl). His research interests include network security, steganography and wireless networks. He is the author or the co-author of 160+ publications including 110 papers and 50+ invited talks. He is the inventor of 3 patents and pending applications.

Piotr Śmietanka holds the B.Sc. degree in telecommunications from the Faculty of Electronics and Information Technology, Warsaw University of Technology, in 2013. His research interests include network routing and security, steganography and wireless networks.