Security of the Distributed Vehicular Broadcast Protocol DV-CAST

Atallah Almasri
Faculty of Informatics Engineering,
Damascus University, Damascus, Syria

Ghassan Chaddoud
Atomic Energy Commission,
P.O. Box 6091, Damascus, Syria

ABSTRACT
Safety applications are one of the most important applications of Vehicular Ad hoc Networks (VANETs), where safety messages are required to be disseminated in a timely manner to all vehicles within a region of interest. Broadcasting is regarded as the most suitable mechanism to disseminate safety messages, where the focus of routing protocols is on rushing message delivery. However, broadcast routing protocols such as the distributed vehicular broadcast protocol (DV-CAST) and Position-aware reliable broadcasting protocol (POCA) suffer from many types of attack such as forging and modification of safety messages, and repudiation of messages' sources. To thwart such attacks, this paper proposes to empower DV-CAST with security mechanisms to ensure integrity, authentication, and source non-repudiation of safety messages using digital signature. Further, a position verification mechanism is used to ensure the correctness of node position information. Furthermore, privacy of vehicles is provided using temporary IDs. Simulation showed that the proposed security mechanisms do not affect the effectiveness of DV-CAST protocol.

General Terms
Computer Science, Information Security, Network Security.

Keywords
DV-CAST, VANET, safety application, authentication, non-repudiation, privacy, security mechanisms.

1. INTRODUCTION
Generally, a Vehicular Ad hoc Network (VANET) is composed of two types of nodes: mobile vehicles that might be moving at a very high speed, and stationary Road Side Units (RSUs) [1]. Inter-node communications are either single hop or multi-hop. There are two types of communication, the first type, vehicle to vehicle communication (V2V), happens between two vehicles. The second type, vehicle to infrastructure (V2I), happens between vehicles and RSUs. The wireless communication is done by using Dedicated Short Range Communication (DSRC) [2]. The transmission range can up to 1 Km.

There are two major categories of VANET applications: safety applications and non-safety applications [3]. Safety applications are regarded as the most important applications of VANETs. The focus in this paper is only on safety applications. In such applications, when an accident occurs, a safety message should be disseminated as fast as possible to warn nearby vehicles about that accident in a very timely manner.

Broadcasting is regarded as the most suitable mechanism to disseminate safety messages, where the focus of routing protocols is on rushing message delivery. However, broadcast routing protocols such as DV-CAST [4] and Position-aware reliable broadcasting protocol (POCA) suffer from many types of attack such as forging and modification of safety messages, and repudiation of messages' sources [1]. Further, vehicle and driver privacy disclosure is a serious one.

To thwart such attacks, broadcast routing protocols should be equipped with security mechanisms to ensure integrity, authentication, and source non-repudiation of safety messages, and privacy of vehicles and drivers. To the best of our knowledge, there does not exist any work that meet such requirements in DV-CAST protocol.

This paper proposes to use digital signature, position verification, and temporary identities in order to meet the aforementioned security requirements for DV-CAST [4]. Digital signature provides the first three services along with a detection mechanism of position information falsification. Assignment of temporary identities and digital certificates is used to provide anonymity of vehicles.

The rest of this paper organized as follows. Section 2 surveys some of related works. Section 3 overviews DV-CAST protocol, lists attacks targeting DV-CAST messages and related security services. Section 4 describes the security solution. Section 5 shows simulation results and evaluation. Finally, Section 6 is a conclusion.

2. RELATED WORKS
A great effort exerted to secure conventional on demand routing protocols for MANets [5]-[8]. Secure Efficient Distance Vector (SEAD) [5], Ariadne [6], and Secure Routing Protocol (SRP) [7] offers security mechanisms that are based on either hash chain or pre-shared keys. Using hash chains might not be suitable for VANETs in some situations due to time constraints related to chain keys disclosure. Further, pre-shred keys require prior knowledge of network nodes. This requirement does not hold in VANETs. Similarly, Ariadne [6] and Authenticated Routing for Ad hoc Networks (ARAN) [8] propose to use digital signature, however both of them do not show how to manage digital certificates. IEEE 1609.2 secures VANET messages using Elliptic Curve Digital Signature and session key-based symmetric encryption [9].

[10] uses TESLA scheme with signed commitment to ensure security services to beacons exchanged between neighboring nodes in VANETs and addresses instant position verification through position prediction. This work does not discuss the case of multi-hop traffic. Further, it does not provide privacy. Instead of using ECDSA to allow recently joining nodes to authenticate TESLA key chain of the beacon source, [11] uses Bloom Filter. In addition, [11] provides privacy using temporary IDs.

Based on AODV (Ad hoc On-demand Distance Vector), [12] proposed 3VSR (Three Valued Secure Routing) routing protocol that provides entity authentication and non-

repudiation at network join of a node, and ensures cooperation among nodes to evaluate trust among them and detect malicious nodes based on sensing-logic. 3VSR does not provide neither privacy nor per message non-repudiation.

3. DV-CAST AND THREATS

This section introduces DV-CAST protocol and outlines main attacks against it. Next, the security requirements that are necessary to stand up to such attacks are presented. Finally, the security mechanisms that are used to provide these services are explained.

3.1 DV-CAST Protocol

Distributed vehicular broadcast (DV-CAST) protocol [4] is a distributed routing protocol that is specifically devised for VANETs. It delivers broadcast messages via multi-hopping in dense and sparse modes. DV-CAST handles broadcast storm and disconnected network problems simultaneously.

DV-CAST allows each node to be aware of its neighboring nodes as part of its local topology information using a neighbor discovery mechanism. Each node periodically transmits one-single-hop hello message containing its position information and heading. Based on the information collected from hello messages, each node distinguishes among neighboring nodes that are behind, ahead of, and in the opposite direction of it.

When an event triggers the sending of a warning message, the message originator includes in the message its ID, a sequence number, its position information, source's position information, and event-related information such as type, time, position and Region of Interest (ROI). The source broadcasts the message in its vicinity. Based on the information of the local topology and the information included within the warning messages, each node receiving the warning message should decide whether the message is intended to it, to be ignored, or to be rebroadcast. In case it decides to broadcast it, the node replaces the sender's ID and position information by its won data in the message header and then rebroadcasts the message. The message continues hoping until reaching the boundary of the ROI specified in the message.

3.2 Security Attacks

Due to broadcasting and wireless nature, DV-CAST protocol might be susceptible to the following attacks:

- Fabrication Attack. An attacker can initiate this attack by injecting forged messages into the network with a spoofed identifier [1].
- Alteration attacks. It is important to deliver safety messages to all vehicles in a ROI within certain time constraints. Further, it is important to ensure that the warning messages are delivered without modification. If the attacker, or an intermediate node, modifies the message content then the reception of the message would be futile or even harmful.
- Repudiation attack. In normal situations, vehicles participation in accidents must be identified; a source should not be able to deny transmission of safety message [13].
- Location tracking. An attacker can locate and track a vehicle through its transmitted messages – during communication to other vehicles or roadside units. By tracking a vehicle, it becomes possible to build vehicle's profile; in this way, the privacy of the vehicle, and hence, the privacy of the driver is breached [14].
- Position information falsification. Generally, an attacker, a malicious node, can falsify its position in order to cheat other nodes [15]. As it is known, in order to update neighboring tables, each node depends on position information provided from other nodes via Hello and safety messages. Therefore, when an attacker cheats about her/his position information, this directly affects neighboring tables of other nodes. In other words, routing decisions that are taken based on the neighboring table are affected. As a result, falsifying position information affects routing decisions.

3.3 Security Requirements

Generally, confidentially, integrity and availability are major security requirements for any system. However, these requirements may change according to system or protocol characteristics, we claim that the following requirements are sufficient for securing DV-CAST protocol against the aforementioned attacks:

- Authentication. In VANETs, safety applications require efficient authentication mechanism because unauthenticated message may cause threats to human lives [14]. Therefore, it is needed to authenticate the source and any node that relays the message. Authentication protects against fabrication attack.
- Integrity. It is necessary to protect the accuracy and completeness of safety messages' fields. Integrity thwarts alteration attack.
- Non-repudiation. Vehicles causing accident should not be able to deny transmission of safety messages. Moreover, source non-repudiation is useful to detect malicious nodes (i.e., nodes denying the participation in an accident) [13].
- Privacy. Safety messages contain position and ID information of vehicles, so drivers may wary about their position information and IDs as well [13]. Privacy provides guarantee against location tracking attack, and ID disclosure.
- Detection of position cheating. This service is important to verify position information contained within safety and Hello messages. Detection of misbehaving node protects against position information falsification attack.

3.4 Security Mechanism

Regarding the aforementioned security services, [13] proved that using digital signature is the most convenient mechanism to provide authentication, integrity, and non-repudiation in VANETs. However, managing digital certificates in such environment is an issue, especially when the privacy matters.

In addition, classical security mechanisms can not help counter misbehaving nodes [14]. Despite the advantages of digital signature, however it does not guarantee the correctness of position information where the attacker can falsify her/his position information contained either in Hello or safety messages relayed by intermediate nodes.

To cope with the issue of position information falsification, [15] suggested a generic mechanism based on reputation. The reputation is formed and updated over time through direct observations and information provided by other nodes in the network. [16] use the concept of reputation system proposed in [15] and customize it to verify the correctness of position information in geographic ad hoc routing based on many

types of autonomous sensors such as Acceptance Range Threshold (ART) and Mobility Grade Threshold (MGT) sensors. Based on time-dependent observations collected by the sensors of node B (the receiver) and position information received from node A (the sender), node B can calculate a trust value of A, and then makes a decision regarding A's position information.

As for privacy, it is known that each vehicle has an ID, and this ID should be known to the network and at the same time, it should not be possible for any malicious node to misuse it. This paper proposes to assign temporary identities and certificates to vehicles at the very beginning of their join to the VANET.

4. SECURITY OF DV-CAST

A secure version of DV-CAST protocol that can withstand against the attacks discussed in subsection 3.2 is proposed. The mechanisms that are proposed to use are digital signature based on temporary certificates, ART sensors-based position verification, and temporary identities. The following demonstrates how to assign temporary certificates and IDs, and describes how to use them within DV-CAST.

4.1 Temporary ID and Certificate Assignment

It is fair enough to assume that each vehicle is equipped with a permanent ID and digital certificate. The certificate authority that issues those certificates is known to and trusted by VANET operator. These certificates are called, hereafter, permanent certificates.

Further, it is assumed that a VANET covers a certain geographic area, say a highway or a city. At the entrance points, there exist RSUs, named online certificate authorities (OCAs), which will be responsible for granting temporary IDs and certificates. Furthermore, it is assumed that each OCA has a digital certificate announced with periodic beacons. The beacon contains the following: VANET's ID, OCA's ID, OCA's position information, OCA's certificate, and digital signature covering precedent data.

When a vehicle gets closer to the VANET and captures a beacon, *i.e.*, it gets into VANET coverage area, it requests a temporary ID and certificate as follows:

1. The vehicle verifies the authenticity of the beacon using OCA's digital signature.
2. The vehicle then forms a temporary certificate request. The request contains the vehicle's ID, permanent certificate, new public key, and digital signature. The request is protected using the OCA's public key. We denote by temporary public key the key to be included within the temporary certificate, and related private key by temporary private key.
3. Upon reception, the OCA decrypts the request and verifies the vehicle's permanent certificate. In case of successful verification, the OCA generates a temporary ID and online certificate containing the vehicle's temporary ID and public key, and sends them back to the vehicle included within a response. The response is encrypted using the vehicle's public key. In addition, the OCA stores in a table the mapping between permanent certificates and temporary ones.
4. The vehicle decrypts the response, verifies the signature, and extracts the temporary ID and certificate.

The temporary certificate, private key and public key will be used by the vehicle during its join to the VANET. The validity period of a temporary certificate is specified by the OCA and stored inside the temporary certificate. This validity period should cover a join session covering an epoch of time equivalent to the time required by the vehicle to cross the coverage area of the VANET.

4.2 Digital signature and position verification

As mentioned above, digital signature is used to provide message authentication, integrity and non-repudiation to hello and safety messages. However not only the message source has to sign the message but also intermediate nodes. This due to the fact that prior to safety message rebroadcast, each intermediate node replaces sender's ID and position information with its own data. In addition, every receiving node might take action and change its neighbor table based on received hello and safety messages. Precisely, the receiving node makes use of event information and position information of the sender that is a neighbor node.

What we propose is to make the message source signs the message. The receiving node verifies the signature, verifies the position information, and, in case of message rebroadcast, it replaces the sender's signature by its own signature. The following details this procedure.

A vehicle, that has to originate a warning message, uses its temporary private key to generate two signatures: source signature and sender signature. Further, the vehicle adds its temporary certificate as shown in Figure 1. The source's signature is used to protect the event information. The sender's signature covers the whole message.

Any node, that receives the message, proceeds as in the following order. The node verifies:

1. the validity of the sender certificate;
2. the sender signature;
3. sender's position information;
4. validity of the source certificate;
5. the source signature;
6. source's position information.

If all the precedent steps result in successful verification, the node carries on proceeding as specified in DV-CAST. In case of failure of any of the preceding steps, the node ignores the message. When the receiving node is a neighbor of the message source, *i.e*, sender ID and source ID are identical; it only carries out the first three steps. In addition, the node updates its neighbor table.

When the node has to rebroadcast the message, it continues with following steps:

7. It replaces sender's ID and position information by its won data.
8. It generates a signature covering the whole message.
9. It adds the signature and its temporary certificate to the message.
10. It then rebroadcasts the message.

As for the hello message, it only contains the source signature covering the whole message and the source's certificate as

well.

5. ANALYSIS AND PERFORAMCE EVALUATION

This section discusses how the proposed scheme meets the security requirements: privacy, authentication, integrity, and non-repudiation. It is then shown how simulations are used to evaluate the impact of the proposed mechanisms on the performance of DV-CAST.

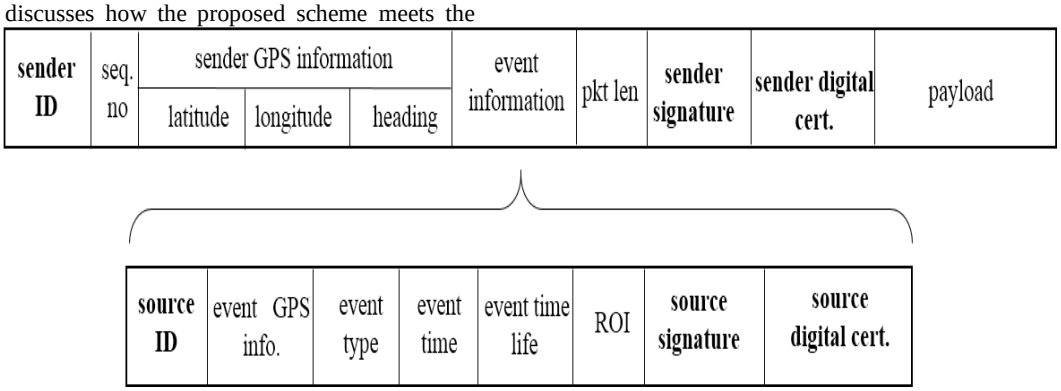

Figure 1. Secure DV-CAST message format.

5.1 Security Analysis

What interests us most is the provision of the privacy of vehicles during their join sessions to the VANET, *i.e.*, tracking their positions and the IDs disclosure should be prevented. In addition, it is required to provide authentication, integrity and non-repudiation.

5.1.1 Privacy.

Prior to VANET join, the vehicle asks for a temporary ID and certificate. The request is protected using the OCA's public key. Further, the related response containing the temporary ID and certificate is protected using the vehicle's public key forming part of its permanent certificate. Moreover, this public key along with vehicle ID will be revealed only to the OCA. No other entity would be able to know any thing about the vehicle ID. In addition, only the OCA knows about the relationship between the permanent IDs and temporary ones.

5.1.2 Authentication and Integrity.

Any node that is the originator or forwarder of a safety message, signs the message using its temporary private key. Further, any node that receives the message verifies the signature using the signer's temporary certificate. Furthermore, any intermediate node adds its own coordinates and signature to the message. The reason for the intermediate signature is that nodes adds their own ID and position information and each node receiving the message updates its local topology or takes decision based on the received information.

5.1.3 Non-repudiation

As long as the RSUs stores signed safety messages and the mapping between permanent and temporary certificates, no node will be able to deny being the source or sender of any message.

5.2 Performance Evaluation

In this work, simulation is used to prove that the security mechanisms do not affect the effectiveness of DV-CAST. We used the "3-second rule" to determine the safety distance between two vehicles heading in the same direction. It is acceptable to say that DV-CAST is still effective if it succeeds to deliver safety messages from a source node to follower nodes that are situated at a distance that is greater than the safety distance within a RIO. In other words, DV-CAST is still capable of delivering safety messages to nodes respecting the 3-second rule with a reasonable delay.

To this end, secure DV-CAST has been implemented in ns 2.35 simulator [17]. We used [18] Crypto++ Library [18] for digital signature. Table 1 lists simulation parameters. In addition, ART sensors are used to verify position information of the sender and source.

It is worth mentioning that temporary IDs and certificates are not implemented.

Table 1. Simulation parameters

Parameter	Value
Simulation area	5000 * 5000 m
MAC protocol	802.11
Simulation time	10 s
Nodes number	40; 124; 248
Node speed	[24 – 30] m/s
Transmission range	550 m
ROI	2500 m

The simulation ran in three different node density to simulate dense, sparse, and totally disconnected network, and evaluated the distance travelled by safety messages with and without security mechanisms. Figures 2, 3 and 4 show simulation results when node density is 40, 124, 248 nodes respectively. We can see that for the three densities, the delay imposed by the security mechanism is barely noticeable and does not affect message delivery to nodes that are close to the message originator. Further, within high node density the messages reach the end of the ROI in less than 150 ms, which is much smaller than 3000 ms. Furthermore, at lower node densities, the distance travelled by messages decreases as the node density diminishes due to the store-carry-forward mechanism [4]. Furthermore, at three seconds, the distance travelled by messages does not vary more than 100 m with or without security services.

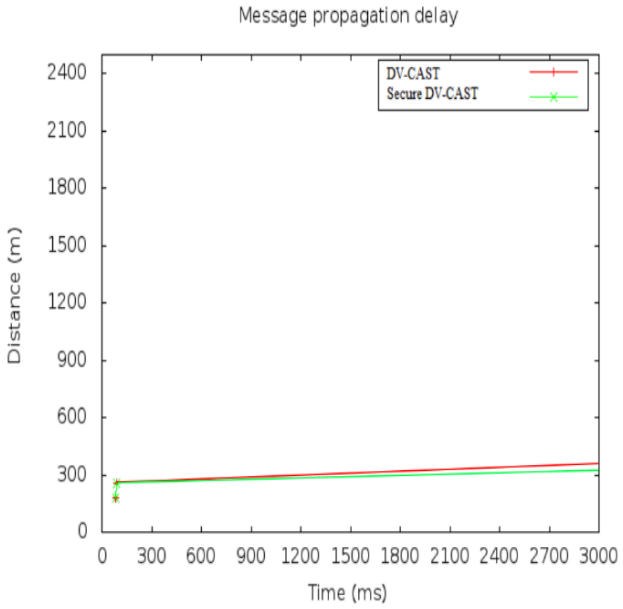

Figure 2. Travelled distance of safety messages for 40 nodes.

6. CONCLUSION

This paper investigated the security attacks against DV-CAST protocol, and presented the security requirements essential for securing DV-CAST against these attacks. The proposed mechanisms ensure authentication, integrity and non-repudiation of safety messages, and vehicle privacy. The later one is provided without using cryptography. The simulation showed that the proposed scheme does not influence DV-CAST effectiveness.

The simulation does not take into account the use of temporary IDs and certificates, in the future it is intended to carry out further specification validation and performance evaluation.

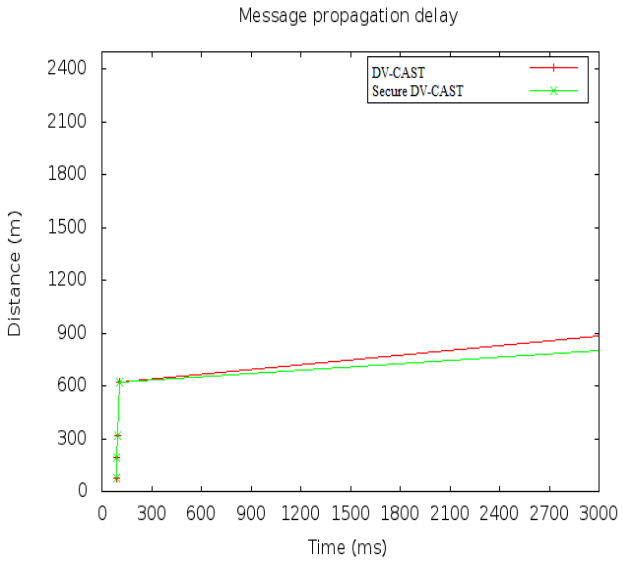

Figure 3. Travelled distance of safety messages for 124 nodes.

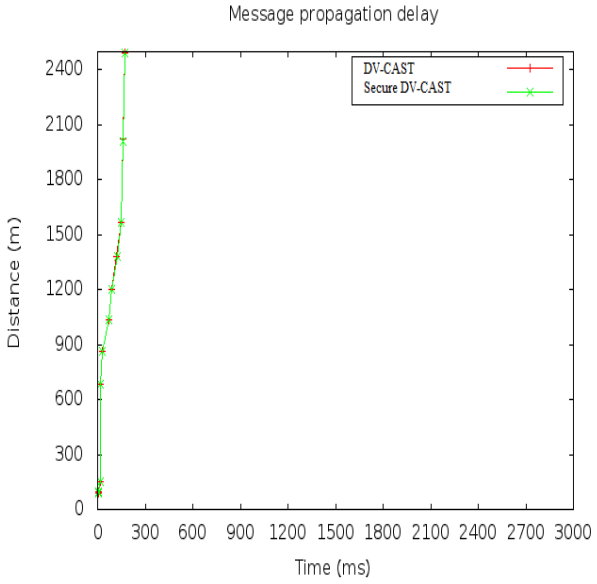

Figure 4. Travelled distance of safety messages for 248 nodes.

7. REFERENCES

[1] G. Samara, W. A. H. W. Al-Salihy, R. Sures, (2010) "Security Analysis of Vehicular Ad Hoc Networks (VANET)", 2010 Second International Conference on Network Applications, Protocols and Services, DOI: http://10.1109/NETAPPS.2010.17

[2] J. B. Kenney, (2011) "Dedicated Short-Range Communications (DSRC) Standards in the United States", Proceedings of the IEEE, Vol. 99, No. 7, p. 1162 – 1182, DOI: http://10.1109/JPROC.2011.2132790.

[3] S. Yousefi, M. S.M ousavi, and M. Fathy, (2006) "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives", 2006 6th International Conference on ITS Telecommunications: DOI: http://10.1109/ITST. 2006.289012.

[4] O. K. Tonguz, N. Wisitpongphan, and F. Bai, (2010) "DV-CAST: A Distributed Vehicular Broadcast Protocol for Vehicular Ad hoc Networks", IEEE Wireless Communications, Vol. 17, No. 2, pp. 47 – 57.

[5] Y.-C. Hu, D. B. Johnson, and A. Perrig, (2002) "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks", Proceedings Fourth IEEE Workshop on Mobile Computing Systems and Applications, DOI: http://10.1109/MCSA.2002.1017480.

[6] Y.-C. Hu, A. Perrig, and D. B. Johnson, (2005) "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks, Vol. 11, No. 1-2, pp. 21-38, DOI: https://doi.org/10.1007/s11276-004-4744-y

[7] Papadimitratos P., Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", in Proceedings of Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), pp. 193-204, doi:10.1.1.12.2420.

[8] K. Sanzgiri, D. LaFlamme, B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer (2005) "Authenticated Routing for Ad Hoc Networks", IEEE Journal on

Selected Areas in Communications, Vol. 23, No. 3, DOI: http://doi.org/10.1109/JSAC.2004.842547

[9] 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages, IEEE, 2016, DOI: 10.1109/ IEEESTD.2016.7426684

[10] C. Lyu, D. Gu, Y. Zeng and P. Mohapatra, (2016) "PBA: Prediction-Based Authentication for Vehicle-to-Vehicle Communications", IEEE Transactions on Dependable and Secure Computing, Vol. 13, No. 1, DOI: https://10.1109/TDSC.2015.2399297

[11] S. Bao1, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo and A. Lei, (2018) "A Lightweight Authentication and Privacy-Preserving Scheme for VANETs using TESLA and Bloom Filters", ICT Express, Vol. 4, No. 4, pp. 221-227, DOI:https://doi.org/10.1016/j.icte.2017.12.001

[12] M. Sohail and L. Wang, (2018) "3VSR: Three Valued Secure Routing for Vehicular Ad Hoc Networks using Sensing Logic in Adversarial Environment", Sensors (Basel), Vol. 18, No. 3, DOI: 10.3390/s18030856.

[13] M. Raya and J. P. Hubaux, (2007) "Securing Vehicular Ad Hoc Networks," Journal of Computer Security - Special Issue on Security of Ad-hoc and Sensor Networks, vol. 15, No. 1, pp. 39-68

[14] B. Mokhtara and M. Azab, (2015) "A Survey on Security in Vehicular Ad Hoc Networks", Alexandria Engineering Journal, Vol. 54, No. 4, pp. 1115-1126, DOI: https://doi.org/ 10.1016/ j.aej.2015.07.011

[15] P. Michiardi and R. Molva, (2002) "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", In: Jerman-Blažič B., Klobučar T. (eds) Advanced Communications and Multimedia Security. IFIP — The International Federation for Information Processing, vol 100. Springer, Boston, MA, pp. 107-121.

[16] T. Leinmuller, E. Schoch and F. Kargl, (2006) "Position Verification Approaches for Vehicular Ad hoc Networks", IEEE Wireless Communications, Special Issue on Inter-Vehicular Communications, Vol. 13, No. 5, pp. 15-21, DOI: 10.1109/WC-M.2006.250353

[17] The Network Simulator, http://www.isi.edu/nsnam/ns.

[18] Crypto++ Library, https://www.cryptopp.com