International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:2, 2016

A Signature-Based Secure Authentication Framework for Vehicular Ad Hoc Networks

J. Jenefa, E. A. Mary Anita

Abstract**—**Vehicular Ad hoc NETwork (VANET) is a kind of Mobile Ad hoc NETwork (MANET). It allows the vehicles to communicate with one another as well as with nearby Road Side Units (RSU) and Regional Trusted Authorities (RTA). Vehicles communicate through On-Board Units (OBU) in which privacy has to be assured which will avoid the misuse of private data. A secure authentication framework for VANETs is proposed in which Public Key Cryptography (PKC) based adaptive pseudonym scheme is used to generate self-generated pseudonyms. Self-generated pseudonyms are used instead of real IDs for privacy preservation and non-repudiation. The ID-Based Signature (IBS) and ID-Based Online/Offline Signature (IBOOS) schemes are used for authentication. IBS is used to authenticate between vehicle and RSU whereas IBOOS provides authentication among vehicles. Security attacks like impersonation attack in the network are resolved and the attacking nodes are rejected from the network, thereby ensuring secure communication among the vehicles in the network. Simulation results shows that the proposed system provides better authentication in VANET environment.

Keywords**—**Non-repudiation, privacy preservation, public key cryptography, self- generated pseudonym.

I. Introduction

VANET is a wireless network in which vehicles are considered as nodes which are mobile in nature. Vehicles communicate with one another to form a network. Communications among vehicles are carried out by using OBU which will be equipped in vehicles by the manufacturers. Due to the mobility of the vehicles, the topology created by the vehicles in the network will be dynamic. VANET has three basic components. They are RSUs, Vehicles and RTA [14]. RSUs are fixed along roadsides which are used to provide services to the vehicles. Network is subdivided into many regions. Each region will be controlled by RTA. Vehicles in a region will be served by assigned RTA and registered RSUs in that particular region. Communications established in VANETs can be classified into three types. They are Vehicle-to-RSU (V2R) communication, RSU-to-Vehicle (R2V) communication and Vehicle-to-Vehicle (V2V) communication.

Vehicular communication plays a vital role in clash avoidance in which vehicles and RSUs are Dedicated Short-Range Communication (DSRC) devices. It works in 5.9 GHz band with a bandwidth of about 75MHz and a range of about 1000m. The main aim of vehicular communication is safety. It allows vehicles to provide information like safety warnings, traffic information, etc. to other vehicles during its travel in a particular region. This information helps the driver to control the vehicle. Vehicular communications are usually developed as a part of Intelligent Transportation Systems (ITS). It helps to achieve safety in an effective way through communications between vehicles and RSUs. It also allows vehicles to share information about traffics which helps them to choose best route to reach their destination.

In VANETs security is a crucial one. Security features like authentication, privacy preservation and non-repudiation play a vital role. Authentication has to be ensured in V2R, R2V as well as in V2V communications which will deny the services to the attackers. Each vehicle has private data which has to be protected. Privacy preservation will avoid the misuse of the vehicle's private data and attacks on their privacy [6]. It should also have a capability to investigate for accidents or liabilities from non-repudiation through which a secure communication among vehicles can be established in a network [1].

II. Related Work

In VANETs security features has its major impact. Different systems are proposed in order to establish a secure authentication framework. Some of the existing systems which provides secure authentication along with privacy preservation and non-repudiation in VANET environment are discussed in this section.

A. Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communication

As detailed in [11], vehicular communications are to be carried out in a secure way. The message which is being transmitted among vehicles has to be traced by the certificate authority in order to recover its original identity. In order to achieve this elliptic curve based chameleon hashing is used. It provides mutual and anonymous authentication, computation efficiency as well as authority tracking capability.

Chameleon signature [3] plays a primitive role in the proposed algorithm. Non-iterative is the uniqueness of chameleon signatures which means the signature can be generated without interacting with the receiver. In this way the performance can be improved to achieve authentication.

The proposed protocol has three phases: registration phase, mutual authentication phase and Certificate Authority (CA) tracking phase. In registration phase OBUs and RSUs will register themselves to CA. During registration CA will

J. Jenefa is currently pursuing Master's degree in Computer Science and Engineering in S.A Engineering College, Chennai, India (e-mail: jene.j6@gmail.com).

E. A. Mary Anita is Professor of Computer Science and Engineering department in S.A Engineering College, Chennai, India (e-mail: drmaryanita@saec.ac.in).

generate and send unique certificates to registered OBUs and RSUs. The next phase involves creating mutual authentication between V2R and V2V. CA tracking phase is used to recover real ID of OBUs and RSUs from their certificates. It provides efficient V2R and V2V authentication with low computation cost and hence it is suitable for realistic vehicular networks.

B. On Joint Privacy and Reputation Assurance (JPRA) for VANETs

JPRA [15] uses a localized model to promote efficient and secure reputation management system. In this model neighbor-certified verification label is introduced which is used by nodes in order to specify its reputation history as well its 1-hop neighbors hold reputation opinions. Different algorithms namely reputation relay algorithm, neighbor-assisted reputation label update algorithm and conditional reputation discretization algorithms are proposed in this model.

Reputation relay algorithm is used to assure that the complete reputation information of a node in the network will be maintained by the node itself and its neighbors in the network irrespective of the topology changes as well as pseudonym changes in the network. Thereby this algorithm achieves reputation management in an efficient way.

Neighbor-assisted reputation label update algorithm helps nodes in the network to update its reputation label whenever necessary. These updates will not affect the pseudonym of that particular node whose reputation label is being updated. Reputation label update of a single node will be reflected in all its neighbor nodes which are at a distance of about 1-hop from the node.

Conditional reputation discretization algorithm permits the legitimate nodes in the network to clear same reputation. This model provides solution to the issues regarding reputation management and privacy-preservation and helps to achieve efficient reputation management as well privacy-preservation in the network. Furthermore, it acquires less computation overhead while achieving both reputation and privacy-preservation.

C. Vehicular Security Through Reputation and Plausibility Checks

As detailed in [7], vehicular security is achieved in this model through reputation and plausibility checks. A secure algorithm is proposed to prevent attacks based on false event generation, event modification, data aggregation and data dropping. It detects the malicious nodes in the network efficiently as well as it removes it from the network. It is a cost efficient approach since only vehicle to vehicle communications are considered in this model. Hence the issues regarding the RSUs are ignored. It is an event oriented approach, since the nodes initiate communication when it observes events in its sensors. It provides security in the network by achieving trust levels for nodes through plausibility checks and reputation. It is mainly proposed to broadcast safety information throughout the network. The information to be broadcast will be transmitted as packets from one node to another through single hop communication and can transmit throughout the network through intermediate nodes by using multi hop communication. In this model, unicast packets will be considered as illegitimate information.

Whenever a node senses an event in its sensor it will forward it to the neighbor nodes. Neighbor nodes can be found through node discovery phase. In this phase, node which senses the event will broadcast Neighbor Req packet and wait for the reply from its neighbors. In this way it discovers the neighbors in the network. Then it will send the packets regarding the event it sensed through its sensors.

Nodes will also monitor its neighbor nodes periodically to determine attackers in the network. It handles four types of attacks as specified by identifying the attackers in the network. After identification, nodes send malicious-intent packet to all its neighbors which have information about the attacker node. Thereby attackers can be detected as well as isolated from the network. Furthermore, it provides secure and robust vehicular security without using any infrastructure.

D. Efficient Privacy-Preserving Authentication for VANETs

In [13], an efficient privacy-preserving authentication scheme is proposed based on group signature. Even though, group signatures are widely used in vehicular networks it has heavy computation delay in Certificate Revocation List (CRL) checking. Hence in this proposed scheme, the area under the coverage of particular network will be divided into several domains. RSUs will disseminate group private keys to these domains. Here Hash Message Authentication Code (HMAC) is used instead of CRL which avoids heavy computation delays.

The proposed scheme has five processes: system initialization, RSU's certificate issuing, vehicle's certificate issuing, secure group key distribution and batch authentication and periodic update of group key. Schnorr signature [8] algorithm is adopted as the primitive algorithm. System initialization involves locating Trust Authority (TA), RSUs and OBUs. Each domain will have many RSUs and OBUs. TA will issue the certificates to RSUs.

Similarly, certificates to vehicles are also issued by TA. The group signature for each domain will be generated along with group public key and they are distributed in the network to all its domains. Group signature verification is carried out by using Wasef and Shen's [12] schemes. Group key can also be periodically updated with the help of TA and RSUs. Different techniques like distributed management, HMAC, batch group signature verification and cooperative authentication are used to achieve a secure authentication scheme. Cooperative authentication is mainly used to improve the efficiency of the proposed scheme. Thereby efficient group signature based authentication scheme is achieved through conditional privacy. Hence the proposed scheme can meet the requirements of verifying large number of messages per second.

E. Securing Warning Message Dissemination in VANETs Using Cooperative Position Verification

A Cooperative Neighbor Position Verification (CNPV) protocol [4] has been proposed. It identifies the nodes which advertising false locations. In this scheme two warning dissemination schemes are used in order to achieve secure vehicular communication. It finds optimal forwarders by ignoring nodes with false locations.

CNPV is a proactive approach, in which the nodes in the network periodically send messages about their locations. It is proposed to achieve two main goals. They are collecting the position of the neighbors and verifying its correctness. It allows the nodes to determine the correctness of the position of its neighbors. It designates each node in three available states. They are verified, faulty and unverifiable.

Verified state describes that the location advertised by neighbor node is true geographic location. Faulty state describes that the location advertised by neighbor node is not true geographic location. Unverifiable state describes that the information obtained from the neighbor nodes are not enough to determine its correctness. Three tests are carried out in verification process. They are Direct Symmetry (DS) test, Cross-Symmetry (CS) test, Multilateration (ML) test. After performing these three tests, nodes will determine whether its neighbors are legitimate forwarders or not. CNPV is easily adaptable to different warning dissemination schemes which use information from neighbors to decide optimal forwarders. It allows nodes to determine the correctness of its neighbor nodes before forwarding the packets.

III. Proposed System

The proposed system is explained by the following process: System Initialization, Pseudo ID generation, V2R and R2V communication and V2V communication. The architecture diagram of the system is shown in Fig. 1. As shown it depicts the overall design of the proposed system. It has RTA which controls a particular region. Whenever a vehicle enters or exits a particular region it first registers itself to the RTA which preloads the ID pools of RSU in that particular region. RTA communicates with RSU through a secure communication as shown. Vehicles communicate with RSU by using its ID and generates offline signature which can be used for authentication among vehicles. By using offline signature vehicles compute online signature and communicate with other vehicles within its range using it. For offline and online signature computation, IBS [9] and IBOOS [10] schemes are used.

A. System Initialization

System Initialization is carried out by using vehicles, RTA and RSUs. RTA controls RSUs present in a particular region by assigning IDs to RSUs. RTA will be responsible for that particular region. Each RSU will be fixed in a particular Home Region. Whenever vehicle enters the region which is under the control of RTA, it registers itself to the RTA. Registration process involves creating a profile for that particular vehicle. Vehicle's Profile has all the original details of the vehicles like license plate number of vehicle, Drivers name etc. During registration process, RTA preloads the IDs of RSU in that region into the vehicles. This helps the vehicle to establish communication with the RSUs.

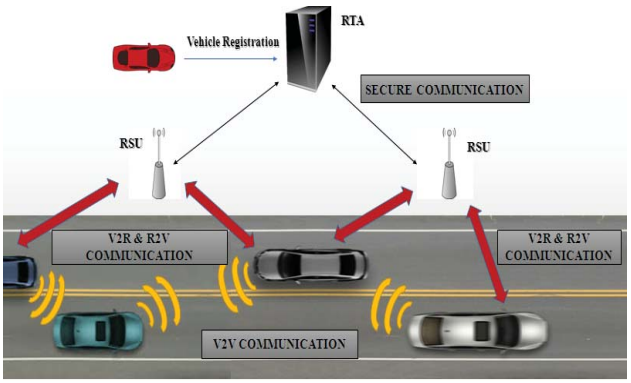

Fig. 1 System Architecture

B. Pseudo ID Generation

After registration, vehicles generate their own pseudo ID which is used instead of real IDs. RTA will broadcast its public key via RSUs periodically. Vehicle in that particular range of RSU will acquire the public key of RTA and use it for pseudonym Generation. It is carried out by using PKC [5] technique. Public key of RTA is used to encrypt the ID of vehicles and pseudo IDs will be created. Pseudo ID of each vehicle is carried out by using:

$$PID_v = T \,||\, E_p(ID_v) \,||\, HM \,||\, ID_{RSU}$$

where PID_v is the pseudo ID of the vehicle, T is the current time, $E_p(ID_v)$is the encrypted value of vehicle's real ID by using RTA's public key acquired from the RSU, HM is the Home Region value of the RSU, ID_{RSU} is the ID of the RSU.

C. V2R and R2V Communication

Vehicles acquire RSU's information that is being periodically broadcast by RSU. After receiving RSU's information, vehicle sends a reply message to RSU for offline signature generation. RSU then computes the offline signature of that particular vehicle by using IBS scheme and broadcasts it to all vehicles in its range.

The steps carried out in the process of establishing V2R and R2V communication is explained in detail below.

Step 1: RSU will be periodically broadcasting its information which will be used by vehicles for offline signature computation. The information which is being broadcast by RSU is given below.

$$<ID_{RSU}, TS, P, M_{ad}, nonce, SIG_{RSU}(ID_{RSU} \,||\, TS)>$$

where ID_{RSU} is the ID of RSU, TS is the time stamp for current time, P is the public key of RTA, M_{ad} is the advertisement message, nonce is for freshness, $SIG_{RSU}(ID_{RSU}||TS)$ is the IBS for R2V authentication which is generated from ID of RSU and time stamp TS.

Step 2: Vehicle acquires RSU's information and sends a reply message for offline signature computation. The reply message send by vehicle to the RSU is of the form given below.

$$<ID_{RSU}, PID_V, TS, JR, SIG_V (PID_V \| TS)>$$

where ID_{RSU} is the ID of RSU, TS is the time stamp for current time, PID_V is the Pseudo ID of vehicle, JR is the join request, SIG_V (PID_V || TS) is the signature generated using Pseudo ID of vehicle and time stamp TS.

Step 3: After receiving the reply message from the vehicle, RSU authenticates the reply message and verifies whether it is a valid signature. If it is a valid one, then it generates offline signature of the vehicle and broadcast it to all the vehicles in its range. The message which is broadcasted to all the vehicles is of the form given below.

$$<ID_{RSU}, TS, set_V(ALL), nonce, SIG_{RSU} (ID_{RSU} \| TS)>$$

where ID_{RSU} is the ID of RSU, TS is the time stamp of current time, set_V(ALL) is the allocation message which is of the form ($PID_V/SIG^{offline}(PID_V)/ID_{RSU}$) is the combination of pseudo ID of vehicle and offline signature which is generated using the Pseudo ID and the ID of RSU, nonce is for freshness, SIG_{RSU} (ID_{RSU} || TS) is the signature generated using the ID of RSU and the time stamp TS.

All the vehicles within the range of RSU accept the message after authentication and store it for further use during V2V communication. In this way V2R and R2V communication is carried out.

D. V2V Communication

Vehicles compute their online signature from the offline signature by using IBOOS Scheme. Vehicle sends authentication message with online signature to all the vehicles within its range. Vehicles verify online signature and accepts the messages if it is valid.

The steps carried out in the process of establishing communication among vehicles are explained in detail below.

Step 1: Vehicle computes the Online Signature from the offline signature generated by RSU. Online signature can be generated by using IBOOS scheme.

Step 2: After computing the Online signature vehicle will send it to all the other vehicles within its range to establish communication. It broadcasts message to all the other vehicles in its range of the form given below.

$$<PID_V, TS, nonce, SIG_V^{online}(SIG_V^{offline}(PID_V)\|TS)>$$

where PID_V is the pseudo ID of vehicle, TS is the time stamp of current time, nonce is for freshness, $SIG_V^{online}(SIG_V^{offline}(PID_V)\|TS)$ is the online signature computed by using offline signature.

Step 3: Vehicles verifies the online signature by comparing it with the offline signature which is stored in its memory. It accepts the message if it is an authenticated vehicle.

In this way communication is established among vehicles in a secured way by using online signature. The expressions used are summarized in a structured format as shown.

Pseudo ID Generation

Step 1: $PID_v = T \| E_p(ID_v) \| HM \| ID_{RSU}$

/* vehicle V generates its pseudo ID */

V2R & R2V Communication

Step 1: RSU → * ; $<ID_{RSU}, TS, P, M_{ad}, nonce, SIG_{RSU} (ID_{RSU} \| TS)>$

/* RSU broadcasts its information to all vehicles within its range */

Step 2: V_v → RSU ; $<ID_{RSU}, PID_V, TS, JR, SIG_V (PID_V \| TS)>$

/* vehicle v sends reply message to RSU */

Step 3: RSU → * ; $<ID_{RSU}, TS, set_V(ALL), nonce, SIG_{RSU} (ID_{RSU} \| TS)>$

/* RSU broadcast to all vehicles in its range */

V2V Communication

Step 1: V_V → V_W ; $<PID_V, TS, nonce, SIG_V^{online}(SIG_V^{offline}(PID_V)\|TS)>$

/* vehicle v authenticates itself to vehicle w*/

IV. Security Attacks

Different types of attacks are possible in vehicular networks [2]. For example, consider Impersonation attack.

A. Impersonation Attack

It is one among the types of attack in which one vehicle acquires the entity of another vehicle and pretends to be another vehicle. During communication attacker can acquire the online signature of one vehicle and communicate with another vehicle using it. In such case, attacker will act as another entity. V2V authentication will identify such attackers and reject it from the network.

The steps involved in verification process are explained in detail below.

Step 1: If a vehicle V uses online signature of vehicle W and tries to communicate with vehicle Z. It sends message to vehicle Z with online signature of vehicle W of the form given below.

$$<PID_V, TS, nonce, SIG_W^{online}(SIG_W^{offline}(PID_W)\|TS)>$$

Step 2: After receiving message from vehicle V, vehicle Z verifies the online signature. It will not match with the offline signature stored in its memory and hence it will identify that vehicle V is an attacker. Then it will send information about the attacker to RSU.

Step 3: Once the attacker vehicle is detected, vehicle Z will send information about the attacker vehicle to the RSU. The information send to the RSU is of the form given below.

$$<ID_V, PID_V, TS, ID_{att}>$$

where ID_V is the ID of the vehicle, PID_V is the Pseudo ID of the vehicle, TS is the time stamp of current time, ID_{att} is the ID of the attacker.

Step 4: After receiving the information about the attacker vehicle, RSU will broadcast about the attacker to all the vehicles in its range. Thereby attacker will be rejected from the network. The message which is broadcasted will be of the form given below.

$$<ID_{RSU}, TS, P, M_{ad}, ID_{att}>$$

where ID_{RSU} is the ID of RSU, TS is the time stamp of current time, P is the public key of RTA, M_{ad} is the advertisement message, ID_{att} is the ID of attacker vehicle.

In this way security attacks in the network can be resolved by using secure authentication framework. Thereby communications among vehicles are carried out in a secure way.

V. Simulation Results

A. Simulation Scenario

The simulations are carried out by creating a VANET environment with one RTA, three RSUs and twenty mobile vehicles moving over a simulation area of 900 x 600 operating space with the simulation time of about 90 seconds. Vehicles will be moving in a random fashion from one position to another with the speed ranging from 0 m/s to 50 m/s. Communications between vehicles will be carried out by sending packets between vehicles with a data transmission rate of about 1Mb. The simulations are carried out with attackers and the attacking nodes are selected randomly.

B. Performance Evaluation

Simulation results are presented by comparing the network scenario with and without authentication. The parameters which are considered for performance evaluation are Delay and Packet Delivery Ratio (PDR). Here, the vehicles are allowed to communicate with other vehicles with and without proposed authentication schemes and the results are observed. The proposed authentication schemes IBS and IBOOS are used for analysis.

C. Delay

The delay in the network specifies the time taken for the packet to transmit across the network from source to destination. It is computed by using:

DELAY=Receiving time-Sending time

It is mainly used to specify how long a packet takes to reach its destination from source. Delay in the network depends on the computations carried out in the authentication. If a particular authentication framework has more computation, then the delay will be more in the network.

Fig 2 shows the variation of delay with respect to time in the network with and without authentication. Delay among the vehicles which send packets to establish communication is graphically depicted. As shown the delay in the network without authentication will be less when compared to that of the network with authentication.

It is shown that the value of delay increases with respect to time. Delay in the network without authentication is 7.8% less when compared to that of the network with authentication. This is due to the additional computation carried out for authentication in the network. Hence the network with less computation has less delay when compared with network with more computation.

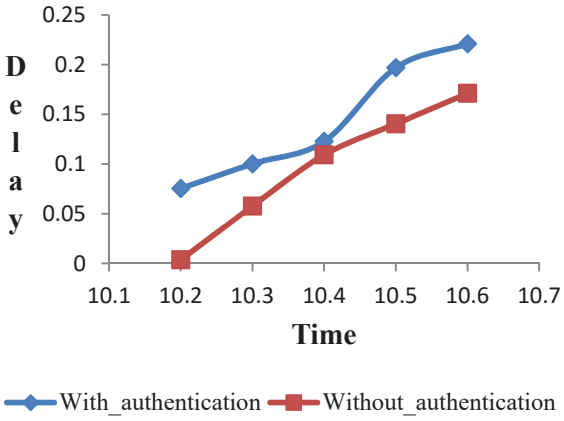

Fig. 2 Delay VS Time

Though the delay is high in the network with authentication it leads to increase in PDR and hence it is accepted. Therefore, there exists a tradeoff between delay and Packet Delivery Ratio in the network.

D. Packet Delivery Ratio

It is the ratio of the number of packets received by the receiver to that of the number of packets sent by the sender. It is calculated by using:

PDR=Sum of packets received / Sum of packets send

It is mainly used to illustrate the level of data delivered to the destination from the source. The greater the value of packet delivery ratio in a network the better will be its performance. The network with secure authentication will have better packet delivery ratio than the network without any authentication.

Fig 3 shows the variation of Packet Delivery Ratio with respect to time in the network with and without authentication in the presence of malicious nodes. PDR for an attacker vehicle which tries to send data to an authorized vehicle with and without authentication is depicted in this graph with respect to time.

As shown in Fig 3, it is clearly understood that the total number of packets received in network with the proposed authentication scheme is 19% more than that of the network without any authentication scheme. Hence it is observed that the PDR for network with proposed authentication scheme is 83% more than that of the PDR for network without any authentication scheme. This is due to the packet loss in the network without any authentication scheme. Hence with

authentication the delivery level of packets to the destination from the source will be more.

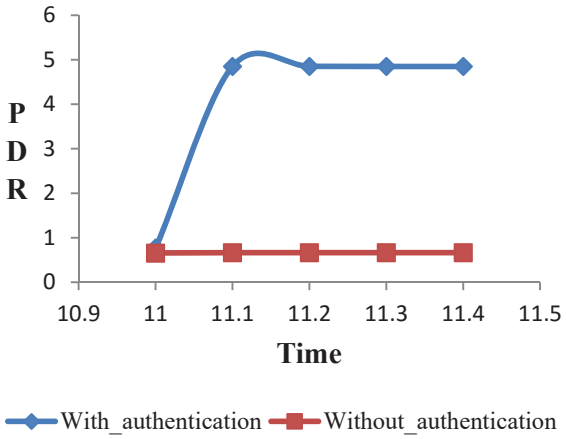

Fig. 3 PDR VS Time

VI. Conclusion

Security in vehicular communication is the major requirement. A secure authentication framework for VANETs has been proposed which uses IBS and IBOOS schemes for authentication purpose between vehicles and RSUs. It provides security features like authentication, privacy preservation and non-repudiation. Simulation result clearly shows that the proposed system provides effective communication by increasing the PDR to 83%. It also shows that the delay in network with the proposed authentication scheme is 7.8% more than that of the network without any authentication scheme. This is due to the additional computation of signatures to establish a secure communication among vehicles. Even though the delay is high, it increases PDR to a certain level and hence it is acceptable. Therefore, a tradeoff exists between delay and PDR in the network. Hence the proposed authentication scheme provides secure vehicular communications. In future, Cross-RSU V2V communication can be proposed which helps vehicles under different RSUs to communicate with one another in a secure way. Attacks based on authentication, security, non-repudiation can also be resolved and attackers can be identified and rejected from the network which ensures secure communication. Selfish nodes in the network can also be identified and rejected. In addition, Cross RTA authentication can also be achieved which establish communication between different RTAs which are responsible for different regions. Thereby vehicle in one region can communicate with vehicles in another region effectively and securely by which additional computation overheads can be reduced and performance of authentication can be improved.

References

[1] F. Armknecht et al., "Cross-Layer Privacy Enhancement and Non-Repudiation in Vehicular Communication," Proc. ITG-GI Conf.Comm. in Distributed Systems (KiVS), pp. 1-12, 2007.

[2] J.M.D. Fuentes, A.I. Gonz_alez-Tablas, and A. Ribagorda, "Overview of Security Issues in Vehicular Ad-Hoc Networks," Handbook of Research on Mobility and Computing, pp. 894-911, IGI Global Snippet, 2011.

[3] H. Krawczyk et al., ''Chameleon Signatures,'' in Proc. Netw. Distrib. Syst. Security Symp. 2000, pp. 143-154.

[4] Manuel Fogue et al., "Securing Warning Message Dissemination in VANETs Using Cooperative Neighbor Position Verification," IEEE Transactions on Vehicular Technology, vol. 64, no. 6, pp. 2538-2550, June 2015.

[5] R.A. Mollin, "RSA and Public-Key Cryptography," Discrete Math. and Its Applications. Chapman and Hall/CRC, 2002.

[6] M. Raya et al., "Securing Vehicular Ad Hoc Networks," J.Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[7] Sanjay K. Dhurandher et al., "Vehicular Security through Reputation and Plausibility Checks", IEEE Systems Journal, vol. 8, no. 2, pp. 384-394, June 2014.

[8] C. P. Schnorr et al., "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.

[9] Shamir et al., "Identity-Based Cryptosystems and Signature Schemes," Proc. CRYPTO, pp. 47-53, 1985.

[10] Shamir et al., "Improved Online/Offline Signature Schemes," Proc. CRYPTO, pp. 355-367, 2001.

[11] Song Guo et al., "Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 2794-2803, November 2014.

[12] A. Wasef et al., "Efficient group signature scheme supporting batch verification for securing vehicular networks," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010, pp. 1–5.

[13] Xiaoyan Zhu et al., "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 907-919, February 2014.

[14] S. Zeadally et al., "Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges," Telecomm. Systems, vol. 50, no. 4,pp. 217-241, 2012.

[15] Zhengming Li et al., "On Joint Privacy and Reputation Assurance for Vehicular Ad Hoc Networks," IEEE Transactions on Mobile Computing, vol. 13, no. 10, pp. 2334-2344, October 2014.