Security Analysis of Discrete Event Based Threat Driven Authentication Approach in VANET Using Petri Nets

Arun Malik[1] and Babita Pandey[2]

(Corresponding author: Babita Pandey)

Department of Computer Science and Engineering, Lovely Professional University[1]
Department of Computer Applications, Lovely Professional University[2]
Jalandhar - Delhi G. T. Road, Phagwara, Punjab 144411, India
(Email: arunmalikhisar@gmail.com)

(Received Nov. 3, 2016; revised and submitted Mar. 31, 2017)

Abstract

Vehicular Ad hoc Network (VANET) is identified as a key part of Intelligent Transport framework. VANET plays a significant role to establish communication between Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Keeping in mind the end goal to build an effective network, it is expected to have steadiness of security and transmission of unwavering quality in VANET. In this paper, a discrete event based threat driven authentication approach to provide secure communication between V2V and V2I is proposed. A combination of re-encryption key, public key, private key and session key is used by this approach for guaranteeing a secure communication between vehicle to vehicle and vehicle to Road side Unit (RSU). The analysis of the proposed approach is realized by using Petri nets and Veins framework. The proposed approach is also compared with the related works on the basis of computational overhead (CO), throughput, packet delivery ratio and average delay. The evaluated results reflect that proposed approach outperforms.

Keywords: Road Side Unit; Vehicle to Infrastructure; Vehicle to Vehicle; Vehicular Ad hoc Network

1 Introduction

VANET act as a promising application situation for facilitating intelligent transport system. In VANET, V2V and V2I are the two types of primary communications [6,7,17]. In VANET vehicles are having their communication devices, through the help of which vehicles initiate communication among themselves and also communicate with the RSUs placed at vital points on the side of road. In V2V communication, the on board unit(OBU) embedded in vehicles frequently broadcast information related to location of the vehicle, speed of the vehicle, present time, direction, acceleration/deceleration of the vehicles and traffic events [12, 18]. Due to which driver can obtain a better-quality understanding of their driving situations. Moreover, with the help of the information frequently broadcasted by OBU, VANET plays a vital role in prevention of accidents, in providing solution for heavy traffic jams and in broadcasting of alternate road messages [13]. On the other hand, vehicles are provided with internet facilities for accessing local information, entertainment, songs and movies in V2I communication [15].

Security and privacy are the major barricades in the successful deployment of VANET [9]. Before utilizing the above attractive applications of VANET, issues related to security and privacy must be resolved. Authentication and integrity of messages exchanged among vehicles and between vehicles and RSUs must be ensured. To provide security and privacy to the information exchanged among vehicles and between vehicles and RSUs, it is very important to establish secure authentication among vehicles and between vehicles and RSUs. Plenty of research work has been done in VANET related to privacy and security preservation based authentication schemes. But most of the existing authentication schemes are vulnerable to various types of attacks in VANET which results in lesser throughput and high computational cost Therefore, to design a secure authentication scheme with high throughput and low computational cost still remains a primary challenging problem in VANET.

Thus primary aim of this paper is to address the authentication problem among the vehicles and between vehicles and RSUs. The authentication among the vehicles and between vehicles and RSUs helps to prevent accidents and traffic jams. Moreover, it can also be utilized as fundamental information for any type of responsibility issue after accident. In order to provide an efficient security mechanism in VANET, this paper proposes a discrete event based threat driven authentication approach. Performance of the proposed approach is analyzed by using Petri net model and veins framework.

The remainder of this paper is organized as follow. Section 2 describes the related work. Next, Section 3 describes the methodology of proposed authentication approach. Section 4 describes the petri net model of the proposed authentication approach. Section 5 describes the system model used to simulate the proposed authentication approach. Results and discussions are described in Section 6 before concluding the paper in section 7.

2 Related Works

This section describes in brief the different types of existing authentication schemes in VANET.

In [10] to diminish the entrust of authentication delay, an authentication scheme is proposed that utilize a process based on dynamic session secret to increase the computational efficiency and speed of authentication procedure. This scheme has efficient authentication ability and safeguards the VANET towards variety of malicious attacks.

In [11] an efficient authentication protocol is proposed to provide an anonymous authentication that utilize certificate less signcryption without pairing. Even in the absence of RSU, the proposed protocol performs efficiently.

In [14] an exhaustive message authentication scheme is proposed that provide authentication among inter RSU ranges and between Intra RSU ranges. This authentication scheme also permits the hand off among different RSUs. This scheme provides an efficient secure communications by balancing the computational overhead.

In [4] a trust evaluation mechanism is utilized to calculate trust value for the nodes. The trust values assigned to nodes are useful in identifying the malicious nodes in the network. Moreover, a layered structure is demonstrated to establish communication among the authenticating vehicles.

In [5] a novel and efficient authentication method is proposed to provide authentication to public and private vehicles in VANET. To speed up the process of many to one communication, the total signature and total signcryption are utilized.

In [16] an authentication protocol based on blind signature scheme is proposed for I2V communication. This authentication scheme not only provide speedy authentication but also assure the security and location anonymity to the vehicle.

In [2] an authentication scheme is described that utilize identity based signature mechanism in a way to provide multiple level of secrecy to vehicles in VANET. This authentication scheme utilizes an efficient pseudonyms issuance mechanism with the help of which pseudonyms issuer can issue unique pseudonyms to the vehicles. Moreover, each pseudonym binds with the expiration date due to which no public key certificate is required by this protocol to implement short term credentials.

In [1] time stamp based authentication approach is proposed to provide authentication among vehicles and RSU. Legal users are protected from malicious attacks with the help of this authentication approach. This authentication approach provides privacy to every vehicle by not revealing the original identity of vehicles.

In [3] a light weight authentication scheme is mentioned that provides authentication among vehicles and RSUs in VANET. This scheme utilizes hash function, XOR operation and symmetric cryptography to provide privacy and security among vehicle and RSU in VANET.

In [8] a novel ID based authentication scheme is proposed to provide secure RSU to Vehicle communication in VANET. For authentication this scheme uses road pass ticket and vehicle plate number. The effectiveness of this scheme is is analyzed by using Petri nets.

The aforementioned conventional authentication schemes discussed so far do not provide the complete authentication solution for VANET. As these schemes either provides authentication among the vehicles or between vehicles and RSUs. None of the aforementioned authentication schemes provides authentication among the vehicles and between vehicles and RSUs together which results in lesser throughput and high computational overhead. Therefore, the authentication approach proposed in this paper provides authentication among the vehicles as well as the authentication between vehicles and RSUs. Thus providing the complete authentication solution for VANET.

3 Proposed Authentication Approach

In this approach, before starting the authentication process among vehicles and between vehicles and RSUs, credential provider provides the credentials related to Vehicle and RSU that enter into the VANET. Credentials includes public key of moving vehicle, private key of moving vehicle, session key, public key of credential provider, re-encryption key of moving vehicle, public key of fixed RSU, private key of fixed RSU, re-encryption key of fixed RSU.

Step by step procedure used for the authentication between vehicle and RSU is as follow:

- Vehicle sends a message containing arbitrary number X1, particular time instance t1, and session key S1. The sent message is first encrypted with public key of fixed RSU that can be decrypted by private key of RSU.

- RSU initiates message transmission to vehicle containing arbitrary number X1 send by vehicle, arbitrary number X2 generated by RSU, Session key S1 and a particular time instance t2. Then, message is encrypted with the public key of credential provider.

- Public key of credential provider plus re-encrypt key of moving vehicle generates public key of moving vehicle. When public key of vehicle is next generated the message is decrypted by the private key of moving vehicle. Arbitrary number X1 generated by vehicle is verified.
- Vehicle sends a message to RSU containing arbitrary number X2 generated by RSU, Session key S1 and a particular time instance t3. The message is then encrypted with the public key of credential provider
- Public key of credential provider plus re-encrypt key of RSU generates public key of fixed RSU. When public key of fixed RSU is generated the message is then decrypted with the private key of fixed RSU. Arbitrary number generated by the RSU is verified.
- Authentication is over after verifying the arbitrary number X1 and X2 by both vehicle and RSU and communication is established.

Step by step procedure used for the authentication between two vehicles is as follow:

- Vehicle V_i sends a message containing arbitrary number X1, particular time instance t1, and session key S1. The sent message is first encrypted with public key of Vehicle V_j that can be decrypted by private key of Vehicle 2.
- Vehicle V_j initiates message transmission to vehicle V_i containing arbitrary number X1 send by vehicle, arbitrary number X2 generated by vehicle V_j, Session key S1 and a particular time instance t2. Then, message is encrypted with the public key of credential provider.
- Public key of credential provider plus re-encrypt key of vehicle V_i generates public key of vehicle V_i. When public key of vehicle V_i is generated the message is decrypted by the private key of vehicle V_i. Arbitrary number X1 generated by vehicle V_i is verified.
- Vehicle V_i sends a message to vehicle V_j containing arbitrary number X2 generated by vehicle V_j, Session key S1 and a particular time instance t3. The message is then encrypted with the public key of credential provider
- Public key of credential provider plus re-encrypt key of vehicle V_j generates public key of vehicle V_j. When public key of vehicle V_j is generated the message is then decrypted with the private key of vehicle V_j. Arbitrary number generated by the vehicle V_j is verified.
- Authentication is over after verifying the arbitrary number X1 and X2 by both vehicle V_i and vehicle V_j and communication is established.

Algorithms for establishing mutual authentication are listed in Algorithms 1 and 2.

Algorithm 1 Authentication between Vehicle and RSU

```
Begin
Initialize the authentication. .
while Authentication session not end do
    Vehicle send message containing(X1,S1, t1) encrypted with public key of RSU
    RSU Decrypts the message by its private key.
    RSU then send the message containing (X1,X2,S1, t2) encrypted with public key of credential provider.
    Public key of Vehicle⇐public key of credential provider + re-encryption key of vehicle
    Vehicle decrypts the message by its private key
    if X1 in the message send by RSU to the vehicle matches with theX1 genrated by vehicle then
        X1 verified
    end if
    Vehicle send the message containing (X2,S1, t3) encrypted with public key of credential provider.
    Public key of RSU⇐public key of credential provider + re-encryption key of RSU
    RSU decrypts the message by its private key
    if X2 in the message send by vehicle to the RSU matches with theX2 genrated by the RSU then
        X2 verified
    end if
    Establish communication between Vehicle and RSU
end while
End
```

Algorithm 2 Authentication between Vehicle V_i and Vehicle V_j

```
Begin
Initialize the authentication. .
while Authentication session not end do
    $V_i$ send message containing(X1,S1, t1) encrypted with public key of $V_j$
    $V_j$ Decrypts the message by its private key.
    $V_j$ then send the message containing (X1,X2,S1, t2) encrypted with public key of credential provider.
    Public key of $V_i$ ⇐public key of credential provider + re-encryption key of $V_i$
    $V_i$ decrypts the message by its private key
    if X1 in the message send by $V_j$ to the $V_i$ matches with theX1 genrated by $V_i$ then
        X1 verified
    end if
    $V_i$ send the message containing (X2,S1, t3) encrypted with public key of credential provider.
    Public key of $V_j$ ⇐public key of credential provider + re-encryption key of $V_j$
    $V_j$ decrypts the message by its private key
    if X2 in the message send by $V_i$ to the $V_j$ matches with theX2 genrated by the $V_j$ then
        X2 verified
    end if
    Establish communication between $V_i$ and $V_j$
end while
End
```

4 Petri Net Model for Proposed Authentication Approach

Petri net is widely used in depicting the dynamic behavior of system due to its simple and flexible nature. Petri net can be applied to variety of systems in the form of graphical and mathematical modeling tool. Petri net is capable tool to illustrate and learn information processing systems that are described as being synchronous, asynchronous, parallel, distributed, non deterministic, and/or stochastic. Petri net is utilized to draw flow charts, block diagrams and networks. Moreover, Petri net is used to simulate the lively and synchronized actions of the systems.

A discrete event based threat driven authentication approach for vehicles and RSUs has been proposed in the previous section. The proposed authentication approach is analyzed by using Petri net model that control arbitrary events and processes the input data. Petri net model carries out various types of token values from one place to another at the time of transition firings where initial marking is labeled by P0. The subsequent Petri net model and reachability graph for the proposed authentication approach is shown in Figures 1 and 2 respectively.

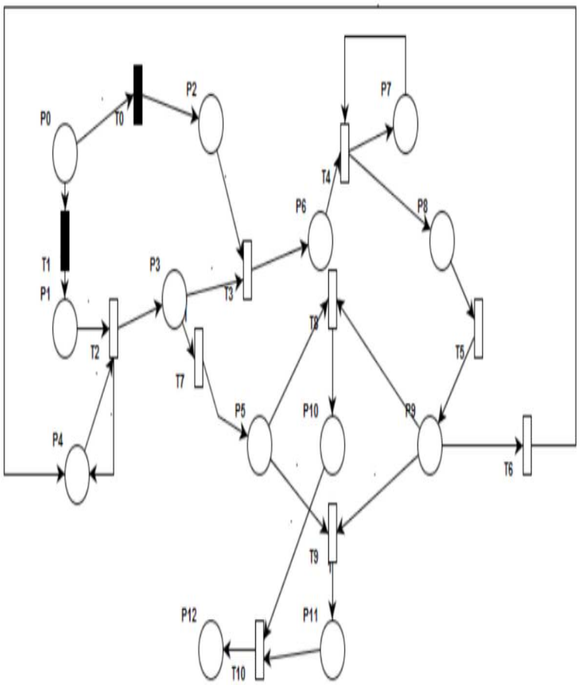

Figure 1: Petri net model for the proposed authentication approach

Reachability and liveness are the two important properties that must be possessed by the proposed authentication approach for the assessment of its correctness. Whether we can reach from one state to another is determined by the reachability. Whether all reachable state can be fired without coming into deadlock situation is determined by liveness. After testing the proposed authentication approach by using Petri net model, it was found that the proposed authentication approach possessed both reachability and liveness properties. Various types of marking and states that can be reached are depicted by reachability graph. In Figure 2 nodes represent markings and arrows are labeled with transition names to represent that markings are reached by firing a certain transitions.

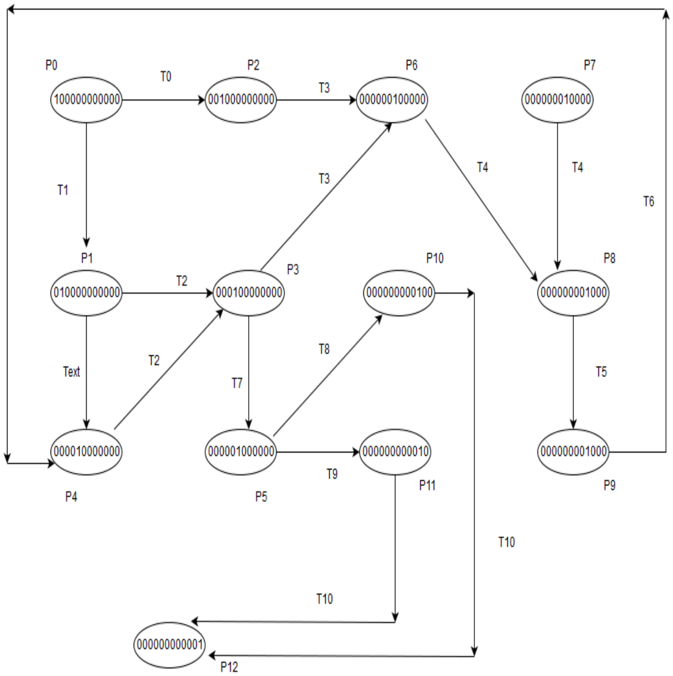

Figure 2: Reachability graph for proposed authentication approach

Table 1: Description of places

State	Description
P0	Working place of credential provider
P1	Original place of on board unit
P2	Original place of RSU
P3	Waiting place
P4	Working place of on board unit
P5	Keep on board unit information
P6	Waiting Place of RSU
P7	Working place of RSU
P8	Waiting place of RSU
P9	Keep information of RSU
P10	Verify information-Yes
P11	Verify information-No
P12	Workplace for authentication

For the better understanding of the Petri nets model for the proposed authentication approach, description of places and transitions used to represent the proposed authentication approach in Petri net model are shown in Table 1 and Table 1. To analyze the model of the proposed approach, Petri nets tool is utilized in Acer laptop with Window 7 environment. The methodology of the proposed model is carried out smoothly in the given simulation environment. The authentication process among vehicles and between vehicle and RSU is carried out initially whenever a vehicle enters the network. Different types of situations that RSUs and Vehicles can undergo during authentication process are identified from T0-T10 transitions.

Table 2: Description of transition

Transition	Description
T0	Receiving credentials of RSU
T1	Receiving credentials of Vehicle
T2	Process data received from vehicle
T3	Received Data from vehicle and RSU
T4	Process data received from RSU
T5	Received RSU data
T6	Process data received from RSU
T7	Received vehicle data
T8	Verify vehicle and RSU data-Yes
T9	Verify vehicle and RSU data-No
T10	data transmission for authentication

5 System Model

The proposed authentication approach is also compared with the authentication schemes mentioned in [1, 3, 8] by using vehicle in network simulation(Veins) framework. Veins is an open source framework suitable for VANET simulation. In Veins framework simulation model is executed with the help of OMNet++ which is an event based network simulator and SUMO which act as a road traffic simulator. The simulation parameters used to execute simulation moodel are mentioned in Tables 3 and 4.

6 Results and Discussions

The performance evaluation of the proposed authentication approach is compared with the existing authentication approach mentioned in [1, 3, 8] on the basis of CO, throughput, packet delivery ratio and average delay.

The excess time or indirect time required by the authentication approach to establish secure authentication among vehicles and between vehicles ans RSUs is termed as computational overhead (CO). Table 5 depicts the comparison of proposed authentication approach with the existing authentication approach mentioned in [1, 3, 8],

Table 3: Traffic simulation parameters

Parameter Name	Value
Number of Vehicles	5,10,15,20,25,30
Maximum Speed	22m/sec
Acceleration	5m/s^2
Deceleration	8m/s^2
Driver Fault	0.5

Table 4: Network simulation parameters

Parameter Name	Value
Network Simulator	OMNet++
Simulation Time	120 sec
Area of Simulation	400 meters x 400meters
Message Size	512 bytes
Simulation Set Up	Random and Cross roads
MAC Protocol	IEEE802.11p
Range of Transmission	300 meters

where RN represents cost of random number generation, HF represents cost of hash function, AE represents cost of executing asymmetric encryption using re-encryption key, SE represents cost of executing symmetric encryption, XF represents cost of executing XOR function.

Due to the use of complex mathematical function by asymmetric algorithms, they are considered to be the slower as compared to symmetric encryption algorithms. But with the existing state of computational technology, security of VANET depends mainly on the size of the keys of its encryption algorithms. With the advancement of technology both symmetric and asymmetric algorithms requires same key size. Moreover security of asymmetric encryption algorithm exists in the security of its private key that cannot be figure out from its public key. In addition to this, asymmetric encryption algorithm requires less number of secret keys as compared to symmetric algorithm. Asymmetric encryption algorithms are efficient for the encryption of short messages to provide security and privacy in VANET. As our proposed authentication approach utilizes asymmetric encryption algorithm and the other authentication approach mentioned in [1, 3, 8] uses symmetric algorithm, hash function and XOR function due to which CO of the proposed authentication approach is less as compared to the existing authentication approach mentioned in [1, 3, 8] as shown in Figure 3.

The number of data packets sent within a given time period over a physical or logical communication channel is termed as throughput. Throughput of the proposed authentication approach is better as compared to the exisitng authentication approach mentioned in [1, 3, 8] as shown in Figure 4.

The ratio of total number of data packets that are suceesfully received to the total number of data packets

Table 5: Comparison table

CO	Proposed Approach	Approach in [1]	Approach in [3]	Approach in [8]
RN	2	3	2	2
Hash Function	0	4	9	2
AE	2	0	0	0
SE	0	2	6	2
XF	0	3	2	2
Total Cost	2RN+2AE	3RN+4HF+2SE+3XF	2RN+9HF+6SE+2XF	2RN+2HF+2SE+2XF

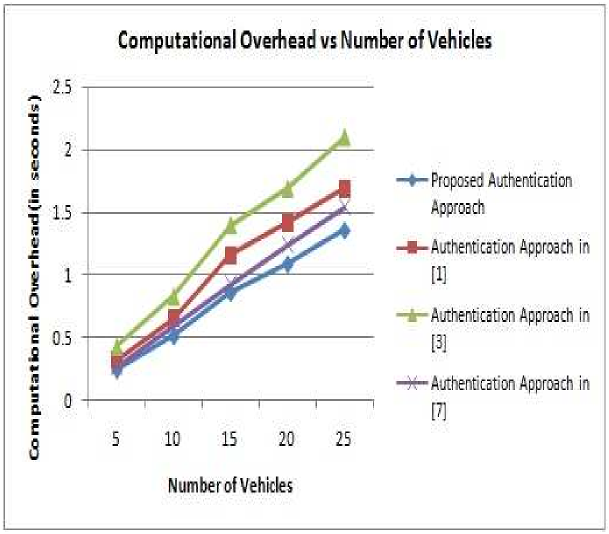

Figure 3: Computational overhead

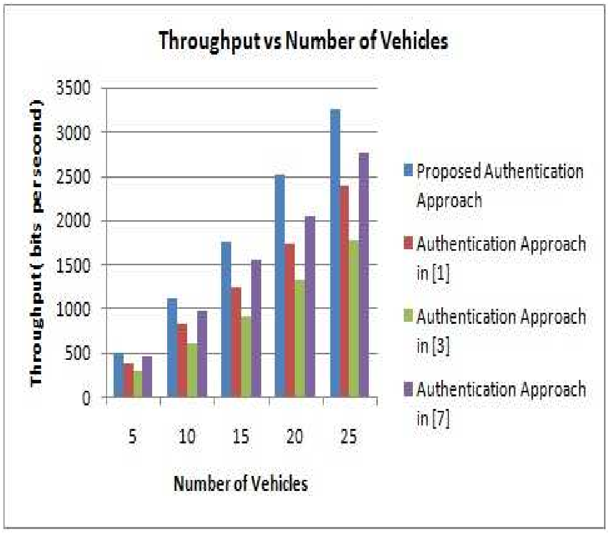

Figure 4: Throughput

sent is termed as packet delivery ratio.Packet delivery ratio of the proposed authentication approach is better as compared to the exisitng authentication approach mentioned in [1,3,8] as shown in Figure 5.

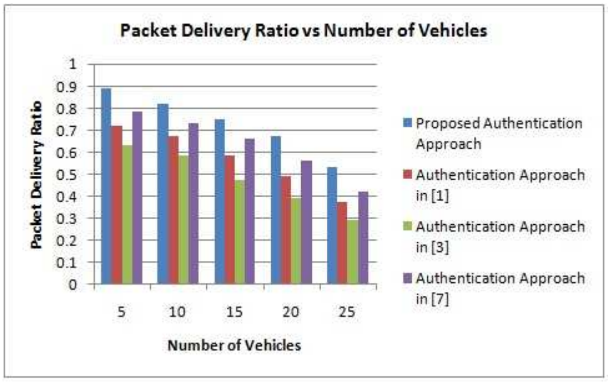

Figure 5: Packet delivery ratio

Time taken by the data packets to reach from source to destination over a given physical or logical communication channel is termed as average delay. Average Delay of the proposed authentication approach is less as compared to the exisitng authentication approach mentioned in [1,3,8] as shown in Figure 6

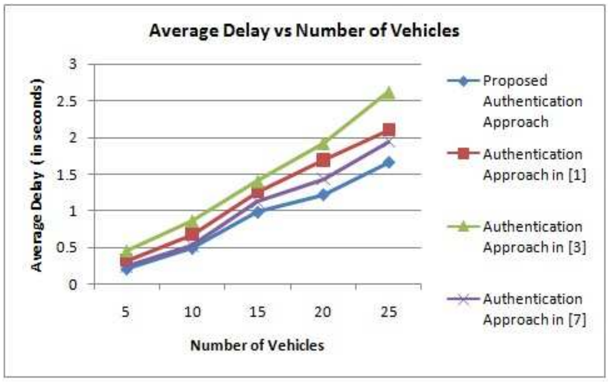

Figure 6: Average delay

7 Conclusions

The discrete event based threat driven authentication approach has been described in this paper. This authentication approach utilizes asymmetric cryptography, reencrypt key and time based arbitrary numbers to provide authentication among vehicles and between vehicles and RSUs. The proposed authentication approach is analyzed by using Petri Nets and Veins framework. With the help of Petri nets model and its reachability graph, it has been observed that the proposed authentication approach acquires the reachability and liveness property. With the help of Veins framework, it has been observed that the proposed authentication approach is better as compared to existing authentication approaches described in [1,3,8] in terms of computational overhead, throughput, packet delivery ratio and average delay. This approach also provides privacy and security among vehicles and between vehicles and RSUs from different types of authentication attacks in VANET.

References

[1] M. Ashritha and C. Sridhar, "Rsu based efficient vehicle authentication mechanism for VANETs," in *IEEE 9th International Conference on Intelligent Systems and Control (ISCO'15)*, pp. 1–5, 2015.

[2] N. B. Bhavesh, S. Maity, and R. C. Hansdah, "A protocol for authentication with multiple levels of anonymity (amla) in VANETs," in *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA'13)*, pp. 462–469, 2013.

[3] M. C. Chuang and J. F. Lee, "Ppas: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks," in *International Conference on Consumer Electronics, Communications and Networks (CECNet'11)*, pp. 1509–1512, 2011.

[4] S. DasGupta, R. Chaki, and S. Choudhury, "Truval: Trusted vehicle authentication logic for VANET," in *Advances in Computing, Communication, and Control*, pp. 309–322, 2013.

[5] Y. Han, D. Fang, Z. Yue, and J. Zhang, "Schap: The aggregate signcryption based hybrid authentication protocol for VANET," in *International Conference on Internet of Vehicles*, pp. 218–226, 2014.

[6] S. Ibrahim, M. Hamdy, and E. Shaaban, "Towards an optimum authentication service allocation and availability in VANETs," *International Journal of Network Security*, vol. 19, no. 6, pp. 955-965, 2017.

[7] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security*, vol. 16, no. 5, pp. 351–358, 2014.

[8] Y. Kim and J. Lee, "A secure analysis of vehicular authentication security scheme of rsus in VANET," *Journal of Computer Virology and Hacking Techniques*, vol. 12, no. 3, pp. 145–150, 2016.

[9] C. T. Li, M. S. Hwang, Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks", *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, July 2008.

[10] J. S. Li and K. H. Liu, "A lightweight identity authentication protocol for vehicular networks," *Telecommunication systems*, vol. 53, no. 4, pp. 425–438, 2013.

[11] R. Pradweap and R. Hansdah, "A novel rsu-aided hybrid architecture for anonymous authentication (rahaa) in VANET," in *International Conference on Information Systems Security*, pp. 314–328, 2013.

[12] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[13] Y. Wang, H. Zhong, Y. Xu, and J. Cui, "Ecpb: Efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs." *International Journal of Network Security*, vol. 18, no. 2, pp. 374–382, 2016.

[14] H. T. Wu and W. S. Hsieh, "Rsu-based message authentication for vehicular ad-hoc networks," *Multimedia Tools and Applications*, vol. 66, no. 2, pp. 215–227, 2013.

[15] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357–3368, 2008.

[16] C. Zhang, R. Lu, P. H. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks," in *Wireless Communications and Networking Conference (WCNC'08)*, pp. 2543–2548, 2008.

[17] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[18] S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, 2015.

Biography

Arun Malik received his Bachelor of Technology from Kurukshetra University in 2008 and Master of Technology from Maharishi Markandeshwar University in 2011.He is pursuing his Ph.D from School of Computer Science and Engineering at Lovely Professional University, Punjab. He has 5 years of teaching experience and published more than 12 papers in journals and conference proceedings.His research interests include wireless networks, Ad hoc Networks, VANET and MANET.

Dr.Babita Pandey is currently with the School of Computer Application at Lovely Professional University, Punjab, India. She obtained her PhD from Indian Institute of Technology-Banaras Hindu University, India in 2009. She has 8 years of teaching experience. She has published more than 80 papers in journals and conference proceedings, some of them are in journal such as such Expert Systems with Applications (Elsevier), Computers in Biology and Medicine (Elsevier), Education and Information Technologies (Springer), SpringerPlus, Nuclear Technology(American Nuclear Society) etc. She is in the editorial board of several journals. Her research interest are intelligent methods in bioinformatics, biomedical signals etc.