CHAPTER 4

SECURITY ANALYSIS OF DISCRETE EVENT BASED THREAT DRIVEN AUTHENTICATION APPROACH IN VANET

In this chapter a threat driven complete authentication approach is proposed that tends to avoid the threats in VANET. The proposed approach provides different set of algorithms used in vehicle to vehicle and RSU to vehicle authentication. This approach is finally analyzed using Petri Nets and performance evaluation is done by taking communication overhead, throughput, packet delivery ratio, and average delay as evaluation parameters.

4.1 Introduction

Conventional authentication schemes discussed so far do not provide the complete authentication solution for VANET. As these schemes either offer authentication among the vehicles moving or between RSUs and vehicles. None of the earlier discussed authentication schemes provides authentication among the vehicles and between vehicles and RSUs together which results in lesser throughput and high computational overhead. Moreover, the existing authentication schemes are still vulnerable to various types of authentication attacks that also affect the network performance. Therefore, an authentication approach is proposed that provides authentication among the vehicles as well as the authentication between vehicles and RSUs. Hence, the proposed scheme provides the complete authentication solution for VANET.

4.2 Proposed Authentication Approach: Methodology

On initial set up during this approach, credential provider distributes the credentials to RSU and vehicle that join the VANET. After that, authentication is performed between RSUs and vehicles and among vehicles. The credentials used in network include public key and private key allotted to moving vehicle, vehicle's session key, credential provider's public key, re-encryption key of moving vehicle,

fixed RSU's public key, fixed RSU's private key, re-encryption key allotted to fixed RSU. The detailed process of step by step authentication between RSU and vehicle is as follow:

- At a specific time instance t_1, vehicle initiate authentication by sending message choosing X_1 as the arbitrary number and S_1 as the session key. Message to be communicated is first encrypted by the fixed RSU's public key which is decrypted using the corresponding RSU's private key.
- RSU now at a specific time instance t_2, initiates transmission of message to vehicle generating its own arbitrary number let's say X_2, arbitrary X_1 received from vehicle, the session key S_1. After that, the full message is encrypted using the public key of credential provider.
- The combination of re-encrypt key provided to moving vehicle and credential provider's public key generates as a result the moving vehicle's public key. Therefore, now message that is appearing as encrypted through the public key of the moving vehicle is decrypted using only the moving vehicle's private key. Vehicle now verifies the X_1 arbitrary number generated by the vehicle.
- At a specific time instance t_3, message is now generated by the vehicle to RSU containing the same S_1 session key, X_2 arbitrary number generated by the RSU. At last, the message is encrypted using public key of credential provider.
- The combination of re-encrypt key of RSU and credential provider's public key generates the public key of fixed RSU. Therefore, now the message that is appearing as encrypted through the public key of the RSU is decrypted using only the fixed RSU's private key. At last, RSU verifies the arbitrary number generated by it.
- After both X_1 and X_2 are verified by vehicle and RSU respectively, authentication is done at both the ends and communication may be initiated now.

The detailed procedure for step by step authentication among two moving vehicles is as follows:

- Taking a specific time instance t_1, an arbitrary number X_1, and a session key S_1, vehicle V_i forms a message. The message sent is first encrypted by Vehicle V_j public key that is decrypted using its private key.
- Next, a message transmission is initiated by vehicle V_j to vehicle V_i where message contains X_2 that is arbitrary number generated by V_j, arbitrary number X_1 that was sent by vehicle V_i, and session key S_1. Finally, applying the public key of credential provider message is encrypted.
- The combination of re-encrypt key given to V_i and credential provider's public key generates vehicle V_i's public key. Therefore, now the message that is appearing as encrypted through the public key of the V_i is decrypted using only the V_i's private key. At last, V_i verifies the arbitrary number generated by it.
- Taking a specific time instance t_3, the arbitrary number X_2 that was generated by V_j is sent by vehicle V_i to vehicle V_j along with the session key S_1. After that, message is encrypted using public key of credential provider.
- The combination of re-encrypt key allotted to V_j and credential provider's public key generates vehicle V_j's public key. Therefore, now the message that is appearing as encrypted through public key of the V_j is decrypted using only the V_j's private key. At last, V_j verifies the arbitrary number generated by it.
- After both X_1 and X_2 are verified by vehicle V_i and V_j respectively, authentication is done at both the ends and communication may be initiated now.

4.3 Algorithms for Establishing Mutual Authentication

4.3.1 Algorithm 1: Authentication between Vehicle and RSU

1: Start
2: Authentication Initialization
3: while session of authentication not come to end do
4: vehicle generates message having (t_1,X_1,S_1) encrypted using RSU's public key
5: Message is decrypted using RSU's private key.

6: RSU generates message having (t_2, X_2, X_1, S_1) encrypted using credential provider's public key.
7: vehicle's re-encryption key + credential provider's public key =>vehicle's public key
8: Message is decrypted using vehicle's private key
9: if X_1 that is generated at vehicle side matches with X_1 sent in the message by RSU then
10: it confirms verification of X_1
11: end if
12: vehicle generates message having (t_3, X_2,S_1) encrypted using credential provider's public key
13: RSU's re-encryption key + credential provider public key=>RSU's public key
14: Message is decrypted using RSU's private key
15: if X_2 that is generated at RSU matches with X_2 sent in the message by vehicle then
16: it confirms verification of X_2
17: end if
18: RSU and vehicle can proceed further with communication
19: end while
20: end

4.3.2 Algorithm 2: Authentication between Vehicle V_i and Vehicle V_j

1: Start
2: Authentication initialization
3: while session of authentication not come to end do
4: V_i generates message containing (t_1, X_1, S_1) encrypted using V_j's public key.
5: message is decrypted using V_j's private key.
6: V_j generates message having (t_2, X_2, X_1, S_1) encrypted using credential provider's public key.
7: V_i's re-encrypt key+ credential provider's public key => V_i's public key
8: message is decrypted using V_i's private key

9: if X_1 that is generated at vehicle V_i side matches with X_1 sent in the message from V_j to V_i then

10: it confirms verification of X_1

11: end if

12: V_i generates message having (t_3, X_2, S_1) encrypted using credential provider's public key.

13: V_j's re-encrypt key + credential provider's public key =>V_j's public key

14: message is decrypted using V_j's private key

15: if X_2 that is generated at V_j matches with X_2 sent in the message by V_i to V_j then

21: it confirms verification of X_2

16: end if

17: V_i and V_j can further proceed for communication

18: end while

19: end

4.4 Petri Net Model for Proposed Authentication Approach

Maintaining the flexible and simple nature, petri net is used widely to represent the dynamic behavior of a system. Petri net works like a mathematical or graphical tool that can be implemented for different systems. Information processing systems that are well known for being distributed, parallel, asynchronous, synchronous, stochastic, and/or non deterministic can be illustrated or learned using petri net tool. Petri net is generally used to design block diagrams, flow charts, and networks. Moreover, to simulate synchronized and lively actions related to a system petri net is used.

An authentication approach that is threat driven discrete event based for RSUs and vehicles has been proposed. Petri net model is used to analyze the proposed authentication approach that helps in processing the input data and to have a control on other arbitrary events. To carry out the different token values at firing of transition from one place to other, petri net model is used where P0 acts as an initial label marking. Petri net model for authentication approach proposed and the corresponding reachability are shown through Figure 4.1 and 4.2 respectively.

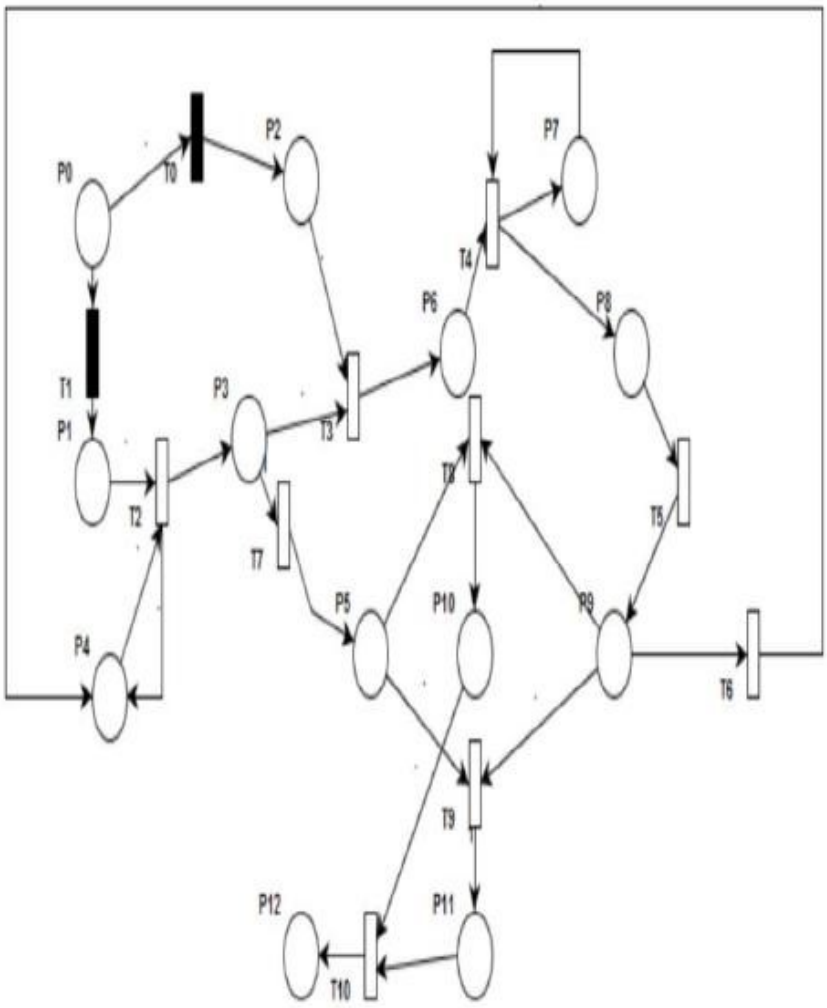

Figure 4.1: Petri Net Model for Proposed Authentication Approach

Correctness of the proposed approach for authentication can be assessed using Reachability and liveliness as its two prime properties. Reachabilty assures that we can move from one state to other. Liveliness is, if all the reachable states do not come to deadlock situation when they are fired. The proposed approach for authentication when tested using Petri net model it possessed both liveliness and reachability properties. Different categories of states and marking that are reached can be represented using reachability graph. In Figure 4.2 markings are represented through nodes and transition names are labeled on arrows to depict that after firing a certain transition the corresponding marking can be reached.

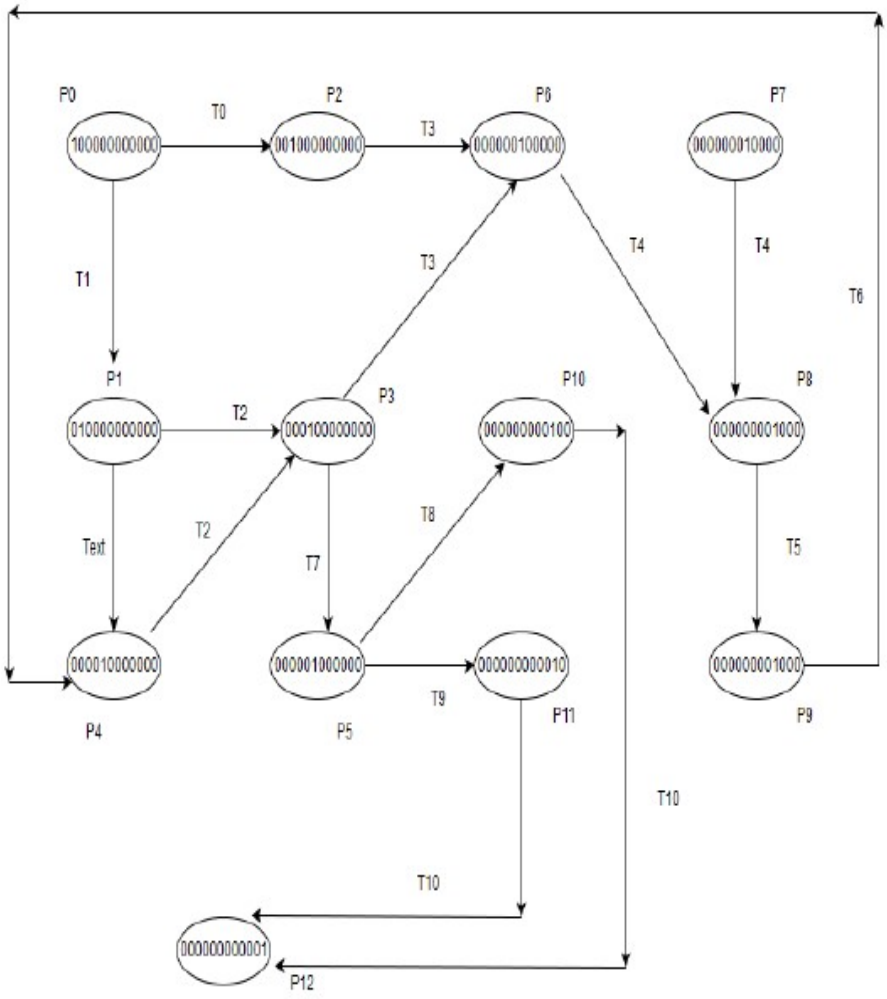

Figure 4.2: Reachability graph for proposed authentication Approach

For choosing the petri nets model for the proposed approach for authentication, description of places and the transitions that are used to represent the proposed approach are shown in Table 4.1 and 4.2 respectively. Petri net model is realized in Acer laptop working on Window 7 environment in order to analyze the proposed approach model. Under the given environment of simulation, the proposed model's methodology worked out efficiently. Whenever a vehicle joins a network, initially authentication is established between RSU and vehicle and among vehicles. Various categories of situations that vehicles and RSUs have to face during authentication are represented from T0-T10 transition as shown in Table 4.2.

Table 4.1: Description of Places

State	Description
P0	Credential provider's working place
P1	On board unit's original place
P2	RSU's original place
P3	Waiting place
P4	On board unit working place
P5	On board unit information is maintained
P6	On board unit information is maintained
P7	RSU's working place
P8	RSU's waiting place
P9	Information of RSU is maintained
P10	Information verified -Yes
P11	Information verified -No
P12	Authentication workplace

Table 4.2: Description of Transition

Transition	Description
T0	RSU's receiving credentials
T1	Vehicle's receiving credentials
T2	Data received from vehicle is processed
T3	Data received from RSU and vehicle
T4	Data received from RSU is processed
T5	RSU data received
T6	Data received from RSU is processed
T7	Vehicle data received
T8	RSU and vehicle data verified –Yes
T9	RSU and vehicle data verified –No
T10	Transmitting data used for authentication

4.5 System Model

Utilizing the vehicle in network simulation (Veins) framework, the proposed approach used for authentication is compared with the existing authentication approaches used in [63], [64] and [65]. For VANET simulation, Veins is considered as an apt framework. The network simulator OMNet++ is used to execute model of simulation in Veins framework and for traffic simulation of road SUMO is used. The parameters taken for simulation in order to execute the model are mentioned in Table 4.3 and 4.4.

Table 4.3: Traffic Simulation Parameters

Parameter Name	**Value**
Number of Vehicles	5,10,15,20,25
Maximum Speed	40 m/s
Acceleration	5m/s2
Deceleration	8m/s2
Driver Fault	0.5

Table 4.4: Network Simulation Parameters

Parameter Name	**Value**
Network Simulator	OMNet++
Simulation Time	1000 sec
Area of Simulation	1000 m x 1000 m
Simulation Set Up	Random and Cross roads
MAC Protocol	IEEE802.11p
Range of Transmission	300 m

4. 6 Results and Discussions

The performance comparison of proposed approach of authentication is made with the existing approaches of authentication mentioned in [63], [64] and [65] in terms of computational overhead, packet delivery ratio, throughput, and average delay.

Asymmetric algorithms are considered relatively slow in contrast to symmetric algorithms due to the use of very complex mathematical functions. Assuming the current age of computational technology, the size of key opted by an encryption algorithm is considered as a major security measure in VANET. In present scenario, asymmetric as well as asymmetric algorithms work on similar key size due to advancement in technology. The fact is, asymmetric algorithm security lies in the strength of its private key which is impossible to get retrieved using its public key. Moreover, the different secret keys required in asymmetric algorithm are less as compared with the symmetric algorithm. To offer privacy and security in short messages, asymmetric algorithms prove to be an efficient encryption in VANET.

The indirect time or the excess time taken by a particular authentication approach to perform authentication among vehicles and among vehicles and RSUs is referred as computational overhead. Table 4.5 illustrates the comparison of existing approaches mentioned in [63], [64] and [65] for authentication with the proposed approach of authentication. In Table 4.5, random number cost generation is represented by RN, hash function cost generation is represented by HF, asymmetric encryption execution cost using the re-encrypt key is represented by AE, symmetric encryption execution cost is represented by SE, XOR function execution cost is represented by XF.

Table 4.5: Comparison of Computational Overhead Parameters for different Authentication Approaches

Computational Overhead	**Approach in [63]**	**Approach in [64]**	**Approach in [65]**	**Proposed Approach**
RN	3	2	2	2
HF	4	9	2	0
AE	0	0	0	2
SE	2	6	2	0
XF	3	2	2	0
Total Cost	3RN+4HF+2SE+3XF	2RN+9HF+6SE+2XF	2RN+2HF+2SE+2XF	2RN+2AE

According to the above table, authentication approach mentioned in [63] has RN as 3, HF as 4, AE as 0, SE as 2, and XF as 3. Authentication approach mentioned in [64] has RN as 2, HF as 9, AE as 0, SE as 6, and XF as 2. Authentication approach mentioned in [65] has RN as 2, HF as 2, AE as 0, SE as 2, and XF as 2. The Proposed authentication approach mentioned has RN as 2, HF as 0, AE as 2, SE as 0, and XF as 0. Therefore the proposed approach has minimum cost as it uses only random number and asymmetric algorithm and no other hash function, symmetric encryption or XOR function is required.

Figure 4.3 represents that computational overhead of the proposed approach of authentication is relatively less in comparison to existing approaches of authentication mentioned in [63], [64] and [65].

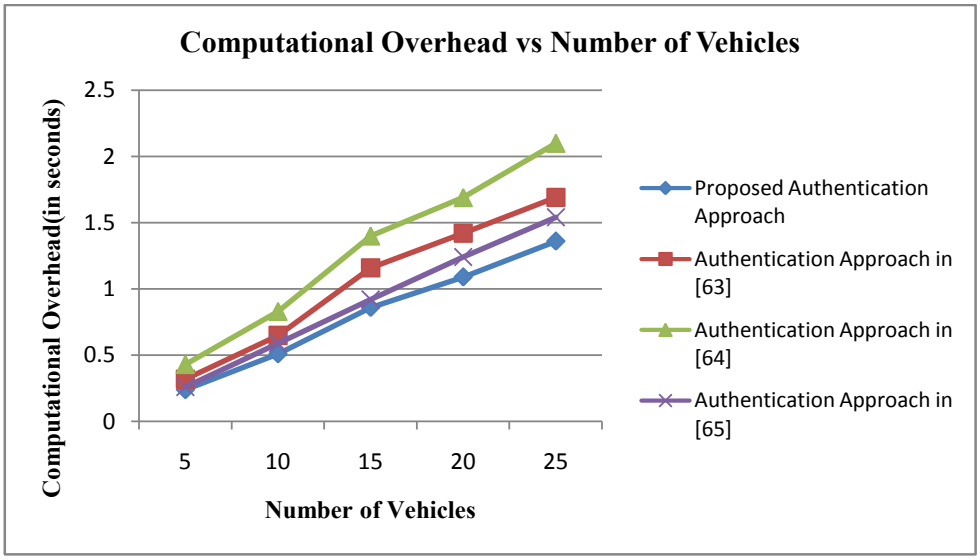

Figure 4.3: Comparison of Computational Overhead for Proposed and Existing Authentication Approaches

The above graph shows that with varying number of vehicles, computational overhead of the authentication schemes also varies. Computational overhead of scheme proposed in [63] is 3% to 13% more as compared to proposed scheme. Computational overhead of scheme proposed in [64] is 7% to 30% more as compared to proposed scheme. Computational overhead of scheme proposed in [65] is 0.3% to 7.2% more as compared to proposed scheme. Therefore, it can be concluded that

proposed authentication scheme performs well with minimum computational overhead even with varying number of vehicles. The existing approaches of authentication mentioned in [63], [64] and [65] uses symmetric algorithm, XOR function, and hash function, whereas, the approach proposed for authentication work on asymmetric algorithm. Therefore, the computational overhead of existing approaches of authentication mentioned in [63], [64] and [65] is more as compared to the proposed approach of authentication.

Over a logical or physical communication channel, the number of packets that are sent within a specific time interval is referred as throughput. Figure 4.4 represents that throughput of the approach proposed for authentication is relatively more as compared to existing approaches of authentication mentioned in [63], [64] and [65].

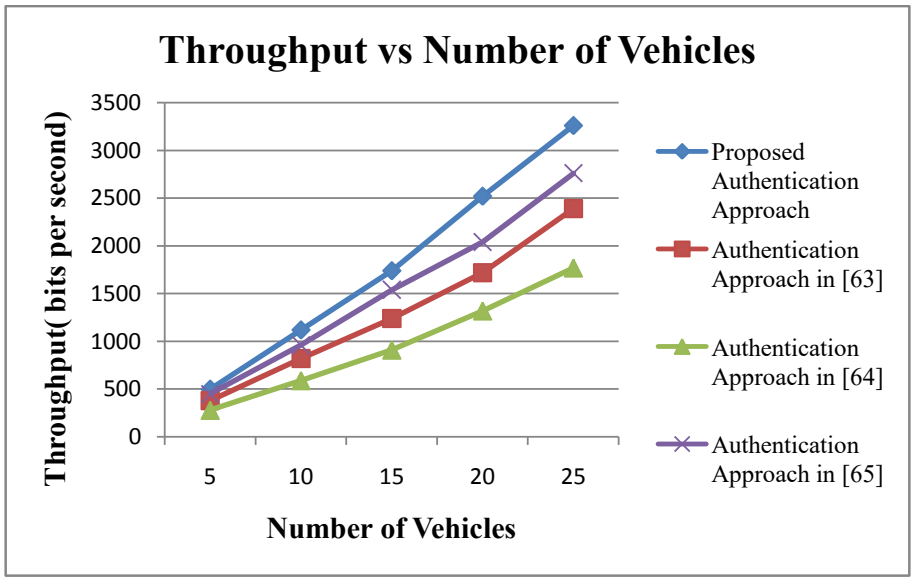

Figure 4.4: Comparison of Throughput for Proposed and Existing Authentication Approaches

The above graph shows that with varying number of vehicles, throughput of the authentication schemes also varies. Throughput of scheme proposed in [63] is 3% to 25% less as compared to proposed scheme. Throughput of scheme proposed in [64] is 6% to 43% less as compared to proposed scheme. Throughput of scheme proposed in [65] is 1% to 15% less as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with maximum throughput even with varying number of vehicles.

Packet delivery ratio is the ratio of the data packets that are effectively arrived at the destination side to the data packets sent from sender side. Figure 4.5 represents that packet delivery ratio of the approach proposed for authentication is high as compared to the existing approaches of authentication mentioned in [63], [64] and [65].

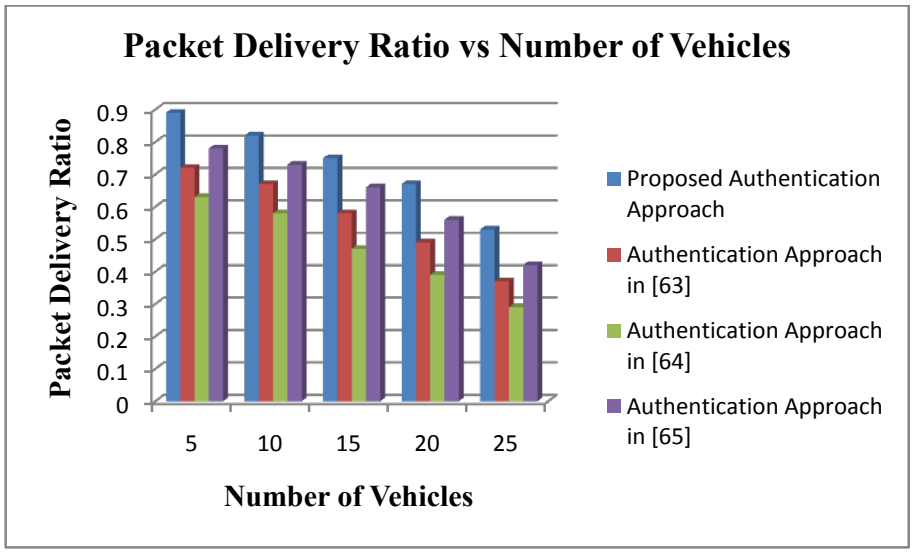

Figure 4.5: Comparison of Packet Delivery Ratio for Proposed and Existing Authentication Approaches

The above graph shows that with the varying number of vehicles, packet delivery ratio of the authentication schemes also varies. Packet delivery ratio of proposed scheme in [63] is 15% to 18% less as compared to proposed scheme. Packet delivery ratio of proposed scheme in [64] is 24% to 28% less as compared to proposed scheme. Packet delivery ratio of proposed scheme in [65] is 9% to 11% less as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with maximum packet delivery ratio even with varying number of vehicles.

Average delay is time elapsed by while sending packet from a specific source to a destination over the given logical or physical communication channel. Figure 4.6 represents that average delay of proposed approach of authentication is less as compared to existing approaches of authentication mentioned in [63], [64] and [65].

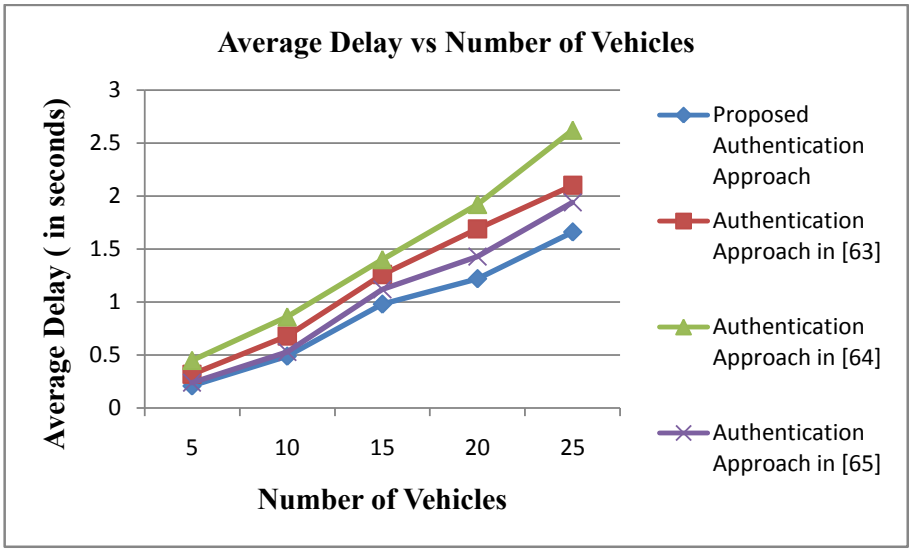

Figure 4.6: Comparison of Average Delay for Proposed and Existing Authentication Approaches

The above graph shows that with the varying number of vehicles, average delay of the authentication schemes also varies. Average delay of scheme proposed in [63] is 3% to 16% more as compared to proposed scheme. Average delay of scheme proposed in [64] is 8% to 32% more as compared to proposed scheme. Average delay of scheme proposed in [65] is 1% to 10% more as compared to proposed scheme. Therefore, it can be concluded that proposed authentication scheme performs well with minimum average delay even with varying number of vehicles.

4.7 Summary

In this chapter, discrete threat driven event based approach for authentication has been proposed. The proposed approach of authentication makes use of asymmetric algorithm, time dependent arbitrary numbers, and re-encrypt key to provide authentication between vehicles and RSUs and among vehicles. Veins framework and Petri Nets are used to analyze the proposed approach for authentication. After analysis through Petri nets model and working on its reachability graph, it has been identified that the proposed approach for authentication pertains the liveness and reachability property. Using the Veins framework it has been observed that proposed authentication approach performs better as compared to existing approaches for authentication detailed in [63],[64], and [65] in terms of computational

overhead, effective packet delivery ratio, average delay, and throughput. It has also been concluded that the proposed approach offers both security and privacy between RSUs and vehicles and among vehicles, preventing VANET from various types of attacks based on authentication.

Once a initial trust is maintained using the efficient process of authentication between the RSUs and vehicles, the next step corresponds to collecting data from the moving vehicles and finally to store that data on RSUs. Next chapter works on detailing the existing schemes for data collection and later an improved scheme is proposed for data collection.