



**EFFICIENT SCHEME FOR RECOGNITION AND EVICTION OF  
SYBIL ATTACK IN VANET**

A Dissertation Proposal  
submitted

**By**

Sagar Narang (11001547)

**to**

**Department of Computer Science & Engineering**

In partial fulfilment of the Requirement for the

Award of the Degree of

**Master of Technology in Computer Science**

**Under the guidance of**

Kundan Munjal (16806)

**(May 2015)**

# ABSTRACT

Vehicular Ad-Hoc Networks (VANET) generalization of Mobile Ad Hoc Networks (MANET) are proclaimed for extreme mobility as compared to MANET. Motivation of VANET is Traffic Administration and Human Protection. Misuse of utilities provided by VANET is more prone to attacks like Black Hole Attack and Sybil Attack. This dissertation is fascinated towards recognition and eviction of Sybil Attack in VANET. In Sybil Attack evil-minded nodes known as Sybil nodes imitate multiple fraud identities of one or more vehicle at same time distorting behaviour of right-minded nodes in network vulnerable to human lives. In this dissertation, different strategies of finding, locating and evicting Sybil Attack in VANET are examined and premised on those examined strategies, effective strategy grounded on RFID, Voting algorithm, Watchdog, single certificate and digital signature is proposed for recognition and eviction of Sybil Attack in VANET. RFID is AIDC technique exerted for automatic identification of vehicles with assistance of RFID tags/reader. Voting algorithm, Watchdog and digital signature are exerted for classification of data as faulty or correct and classification of node as evil-minded or right minded. Digital signatures are exerted for integrity and authenticity of disseminated data. This strategy diminishes spatial, temporal and complexity overhead with allocation of only one certificate to distinct vehicle. With assistance of RFID, vehicle violating utilities and services of VANET through Sybil Attack are easily recognized and evicted. This strategy does not necessitate VPKI and Localization strategies further persuading it as cost-effective resolution to Sybil Attack in VANET by saving spatial and temporal capabilities involved in deployment of storage area and localization devices respectively.

# CERTIFICATE

This is to certify that Sagar Narang (11001547) has completed M.Tech Dissertation-II proposal titled “**EFFICIENT SCHEME FOR RECOGNITION AND EVICTION OF SYBIL ATTACK IN VANET**” under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and partial fulfilment of the conditions for the award of M.Tech Computer Science and Engineering.

Date:

Signature of Advisor

Name:

UID:

## **ACKNOWLEDGEMENT**

I exert this opportunity to assert sincere appreciation to every single person who encouraged and assisted me throughout dissertation. I am glad for their aspirant and friendly supervision during dissertation. I honestly appreciate them for sharing their straightforward and enlightening opinions on various issues associated with dissertation.

I assert sincere appreciation to Mr. Kundan Munjal for his encouragement and supervision in dissertation.

# DECLARATION

I hereby declare that the dissertation proposal entitled “**EFFICIENT SCHEME FOR RECOGNITION AND EVICTION OF SYBIL ATTACK IN VANET**”, submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

**Investigator**

**Regn. No. : 11001547**

# TABLE OF CONTENTS

<b><u>CHAPTER</u></b>	<b><u>PAGE NUMBER</u></b>
<b>1. INTRODUCTION</b>	<b>1-10</b>
1.1 Aspects of MANET	1-2
1.2 Applications of MANET	2-3
1.3 Challenges of MANET	3-5
1.4 Attacks in MANET	5-7
1.5 VANET and its applications	7-10
<b>2. REVIEW OF LITERATURE</b>	<b>11-15</b>
<b>3. PRESENT WORK</b>	<b>16-26</b>
3.1 PROBLEM FORMULATION	16-18
3.1.1 Principal emphasis	16-16
3.1.2 What is Sybil Attack	16-18
3.1.3 Issues due to Sybil Attack	18-18
3.2 OBJECTIVES OF STUDY	18-19
3.3 RESEARCH METHODOLOGY	19-26
3.3.1 Principal elements	19-22
3.3.2 Phases of proposed strategy	22-26
<b>4. RESULTS AND DISCUSSION</b>	<b>27-34</b>
4.1 File formats utilized	27-27
4.2 Protocol utilized and revised	28-29
4.3 Other integrations in ns-2	29-29
4.4 NSTK	29-30
4.5 Simulation factors	30-30
4.6 Simulation outcomes	30-34
<b>5. CONCLUSION AND FUTURE SCOPE</b>	<b>35-35</b>
<b>LIST OF REFERENCES</b>	<b>36-37</b>
<b>APPENDIX</b>	<b>38-39</b>

# LIST OF FIGURES

<b><u>FIGURES</u></b>	<b><u>LABEL</u></b>	<b><u>PAGE NUMBER</u></b>
Figure-1	VANET Architecture	9
Figure-2	Sybil Attack	16
Figure-3	Sybil nodes violating services of VANET	17
Figure-4	Digital Signature (Authenticity and Integrity)	22
Figure-5	Flowchart of various phases of proposed strategy	23
Figure-6	RFID acquisition	24
Figure-7	Structure of VANET	24
Figure-8	Structure of sub-network	25
Figure-9	ping.cc	28
Figure-10	ping.h	28
Figure-11	Tk popup box	30
Figure-12	Initial network topology	31
Figure-13	Network topology after 8.1sec	31
Figure-14	Sybil car disseminate message	32
Figure-15	Car2 disseminate message to Car3	32
Figure-16	Throughput	33
Figure-17	Attacker vs Packet Ratio	33
Figure-18	Attacker vs Average Delay	34

# Chapter 1

## INTRODUCTION

---

MANET is generalization of Wireless Ad-Hoc Network (WANET) which is further generalization of Ad-Hoc networks. There is dissimilarity between Ad-Hoc network and MANET that devices associated in Ad-hoc fashion are not necessarily be moving but moving devices associated in Ad-hoc fashion i.e. MANETs will always be Ad-hoc.

MANET is auto-configured architecture-less network sanctioning mobile devices associated in network for circulating information between them without any background architecture [1] [2]. MANETs are proclaimed for their high mobility. In MANET, mobile devices associated with each other through wireless link without any background architecture are sanctioned to move arbitrarily. Various mobile devices disseminate considering proximity of each other. Mobile devices can be router with multiple hosts and wireless dissemination devices. MANET deliver aspects like Autonomous Terminal, Distributed Operation, Multi-hop Routing, Dynamic Network Topology, Fluctuating Link Capacity and Light Weight Terminals [3].

### 1.1 Aspects of MANET

1. **Autonomous Terminal:** In MANET, mobile devices can operate as host and router for processing capability and switching operations respectively.
2. **Distributed Operation:** In MANET, mobile devices cooperate amongst themselves to accomplish essential tasks as needed like routing, switching, relaying, security etc. Due to absence of centralized administration, administration of network is distributed amongst various mobile devices.
3. **Multi-hop Routing:** In MANET, dissemination among two mobile devices which are not directly associated is carried out over number of intermediate devices whose purpose is dispatching information from one device to other device (Hop to Hop).
4. **Dynamic Network Topology:** In MANET, network topology is reformed quickly and randomly due to mobility.
5. **Fluctuating Link Capacity:** In MANET, bit error rates of connection amongst various mobile devices can be extreme. Single end-to-end route can be exerted by



various sessions. Channel over which mobile devices disseminate has issues of noise, fading, interference, low bandwidth, multiple traversal links and heterogeneous link.

6. **Light-weight Terminals:** In MANET, mobile devices with low CPU processing ability, low power storage and small memory size necessitate enhanced techniques to implement computing and dissemination tasks.

## **1.2 Applications of MANET**

MANETs significance is intensifying with applications varying from diverse, extensive, mobile, dynamic networks to limited, stable networks restricted by power source grounded on enhancement of wireless communication and various utilities of MANET including self-configuring network where mobile devices can also act as router, formation and deformation of network on fly at any place and time, flexibility, scalability where more devices can be added in network without difficulty. Enhancement of wireless communication is inception of technologies like Bluetooth, IEEE802.11 and Hiperlan etc. Conventional applications incorporates:

### **1. Tactical Networks**

- TACNET assist military units to renovate their communications, process for information sharing and data exchange.
- TACNETs are managed by various factors like mobility, terrain, communication resources and network characteristics.
- MANET assist in synchronization of military objects moving at high speeds such as fleets of airplanes or ships.

### **2. Emergency Services**

- MANETs are exerted in emergency and rescue services organizations to ensure public protection and well-being like search and rescue operations, disaster relief, bomb disposal, emergency road service, animal control etc.

### **3. Educational Applicants**

- Virtual classroom, virtual conferences, E-learning are example of Educational applicants where MANETs automatically associates various

networks using various computers to disseminate information among students.

- Virtual classroom software applications utilize various synchronous technologies like web conferencing, video conferencing, live streaming etc.
- Virtual classroom produces virtual learning environment for students to provide them E-learning. It can be asynchronous learning which utilize technologies like emails, Wikipedia, HTML documents etc.

#### **4. Entertainment**

- MANETs can be exerted to play multi-user LAN games where one computer is associated over LAN with other computers by forming ad-hoc network among them. Need for speed, counter strike are examples of multi-user LAN games. There are many more multi-user games that can be played over LAN providing entertainment to MANET devices.

#### **5. Location aware services**

- MANETs can be exerted for location based services anywhere at any time. These services accumulate network configuration and location information of particular user and periodically report application when any modification arises in information. These services include follow-on services, information services, contextual advertising, emergency services, security applications, fleet management etc.
- When customers enter inside shopping mall information about discount on various products can be made available to them on their cell phones which provokes them to make final decision.

### **1.3 Challenges of MANET**

Device acceleration, network scalability, waiting time, topography area, unidirectional association, traffic burden, traffic composition, neutralized burden, degree of mobility are crucial circumstances provoking to various challenges of MANET which degrade its performance.

## **1. Routing**

- In MANETs conventional routing algorithms does not effectively operate due to subsequent reasons:
  - Several path breaks due to mobility of intermediate and end devices.
  - Several path breaks due to dynamic network topology.
  - Preserving stable network topological information at all devices requires control overhead which consumes restricted bandwidth due to several adaptations in network topology.
  - Optimum administration of restricted battery life and processing power.

## **2. Security**

- MANETs are immensely endangered to security attacks due to subsequent reasons:
  - Traffic administration is impossible due to inadequacy of central authority.
  - On fly formation and deformation aspect of MANETs at anyplace and anytime, provokes attacker to associate with network efficiently and evade aspects of MANET by attacks like Denial of Service (DOS) attack, Black hole attack, Sybil attack etc.
  - Multi-hop routing aspect of MANET provokes attacker to distort network operations by various attacks due to premises of distributed protocols that all devices are cooperative in coordination process which is eventually untrue in hostile environment.

## **3. Power Consumption**

- In MANETs, there are power issues due to subsequent reasons:
  - Heterogeneity among devices is factor provoking power issues due to different necessities of different kinds of devices.

- Restricted battery power.
- Device power origin may rapidly diminish due to massive dissemination traffic in multi-hop routing.

#### **1.4 Attacks in MANET**

Numerous attacks on MANETs are grounded into two major classification especially passive attack and active attack which are further classified into different kinds of attacks degrading functionalities of MANET.

In passive attack, intruder's objective is surveillance of disseminating devices in network without any alteration of data disseminated among them which further persuades hard recognition of passive attack. Eavesdropping, traffic analysis are illustrations of passive attack.

In active attack, intruder's objective is alteration of data disseminated in network which further persuades easy recognition of active attack. Active attacks are accomplished by internal or external devices of network. Jamming, denial of service (DOS) attack, repudiation, black hole attack, Sybil attack etc. are illustrations of active attacks.

Numerous attacks on MANETs accomplished on distinct layers of TCP/IP model are as follows:

##### **1. Physical layer**

- **Interference**

Interference is deterioration of dissemination among nodes after penetration in proximity of other disseminating nodes.

- **Traffic jamming**

In Traffic jamming, evil-minded nodes recognize and modulate frequency of disseminating nodes in network for squeezing their network with instigation of attacks like DOS attack, flooding etc.

##### **2. Data link layer**

- **Malicious Behaviour**

Malicious nodes hamper routing protocol's utilized in disseminating network by accomplishment of DOS attack, deceptive data insertion in network, Traffic abuse etc.

- **Selfish Behaviour**

Selfish nodes exclude packets or does not incorporate in packet forwarding process for preservation of resources and battery power.

### 3. Network layer

- **Sybil attack**

In Sybil Attack, evil-minded nodes known as Sybil nodes imitates multiple fraud identities of one device at same time distorting behaviour of right-minded nodes in network which further persuades functionalities of MANET.

- **Black hole attack**

In Black hole attack, evil minded nodes interrupt all data packets disseminated to destination node by erroneous advertisement of optimal or shortest route to respective destination node on reception of route request packet from source node.

### 4. Transport layer

- **Session hijacking**

In Session hijacking, evil minded nodes regulate session among certified nodes. Evil minded nodes hijack and manipulate valid session key of certified users through masquerade attack for invalidated retrieval of information and services preserved in their servers or computer systems.

### 5. Application layer

- **Repudiation**

In Repudiation, evil minded nodes refuse after dissemination of data to other nodes in network.

MANETs are employed in areas like military battlefields, emergency search, rescue sites, classroom and convention where instant utilization and effective reformation is necessary and wired network is inaccessible. This dissertation focuses on recognition and eviction of most commonly occurring Sybil attack in VANET vulnerable to human lives.

## **1.5 VANET & its Applications**

VANET generalization of MANET exerts moving vehicles as mobile nodes in MANET for inception of mobile network. Every moving vehicle in VANET can act as wireless router, access point or node for efficient dissemination among vehicles and with nearby roadside units (RSU). Distance between two vehicles for dissemination is 100-300 metres approx. Any vehicle can join VANET for inception of vehicular network. Corps and fire vehicles are first approximated systems exerting this new emerging technology VANET for safety purposes and traffic related problems. The main difference between VANET and MANET is extreme mobility in VANET as compare to low mobility in MANET. Extreme mobility in VANET triggers vehicles to change their topology instantly as compare to mobile devices changing their topology slowly in MANET. In VANET, vehicles connect and move in structured pattern whereas in MANET, mobile devices connect and move in unstructured pattern.

Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, Zig Bee, Satellites, DSRC (Dedicated Short Range Communications) are technologies exerted in VANET. Intelligent Transportation System (ITS) is composed of VANETs. DSRC are unidirectional or bidirectional, short range to medium range communications channels exerted for automation. ITS applications provides services regarding traffic management and sanctions assorted users to be informed, secured and synchronized. Numerous ITS applications are automatic road administration through camera and vehicle overseeing device, emergency vehicle notification system, collision avoidance system through pre-crash notification etc.

There are three major classifications for grouping of VANET applications:

### **1. Safeguard Applications**

Safeguard Applications are determined towards depleting the threats related to road accidents and loss of human lives.

Numerous safeguard applications are discussed below:

- **Collision Risk Warning**

In Collision risk warning, vehicles are notified about of possibility of accidents through information concerning road intersection, vehicle's velocity, vehicle's location, vehicle's speed, road surface etc. accumulated and examined with assistance of sensors or in-vehicle sensors.

- **Control Loss Warning**

In Control loss warning, vehicles broadcast message to neighbouring vehicles which persuades vehicles receiving such messages to devise conclusion which is further notified to transmitting vehicles.

- **Pre-Crash Warning**

In Pre-crash warning, impact of collision is mitigated with services like airbags, actuators etc. For minimization of collision seriousness various services are exerted like notification to vehicle's drivers, pre-controlled brakes, eviction of excessive slack, self-exertion of full or partial break. Situation of collision is estimated with assistance of information exchanged among vehicles and RSU.

All these safeguard applications comes under Collision avoidance system (CAS).

## 2. **Traffic Administration and Oversee Applications**

Traffic Administration and Oversee applications are determined towards refinement of traffic co-operation, co-ordination and motion among vehicles.

Numerous traffic administration and oversee applications are discussed below:

- **Speed Management**

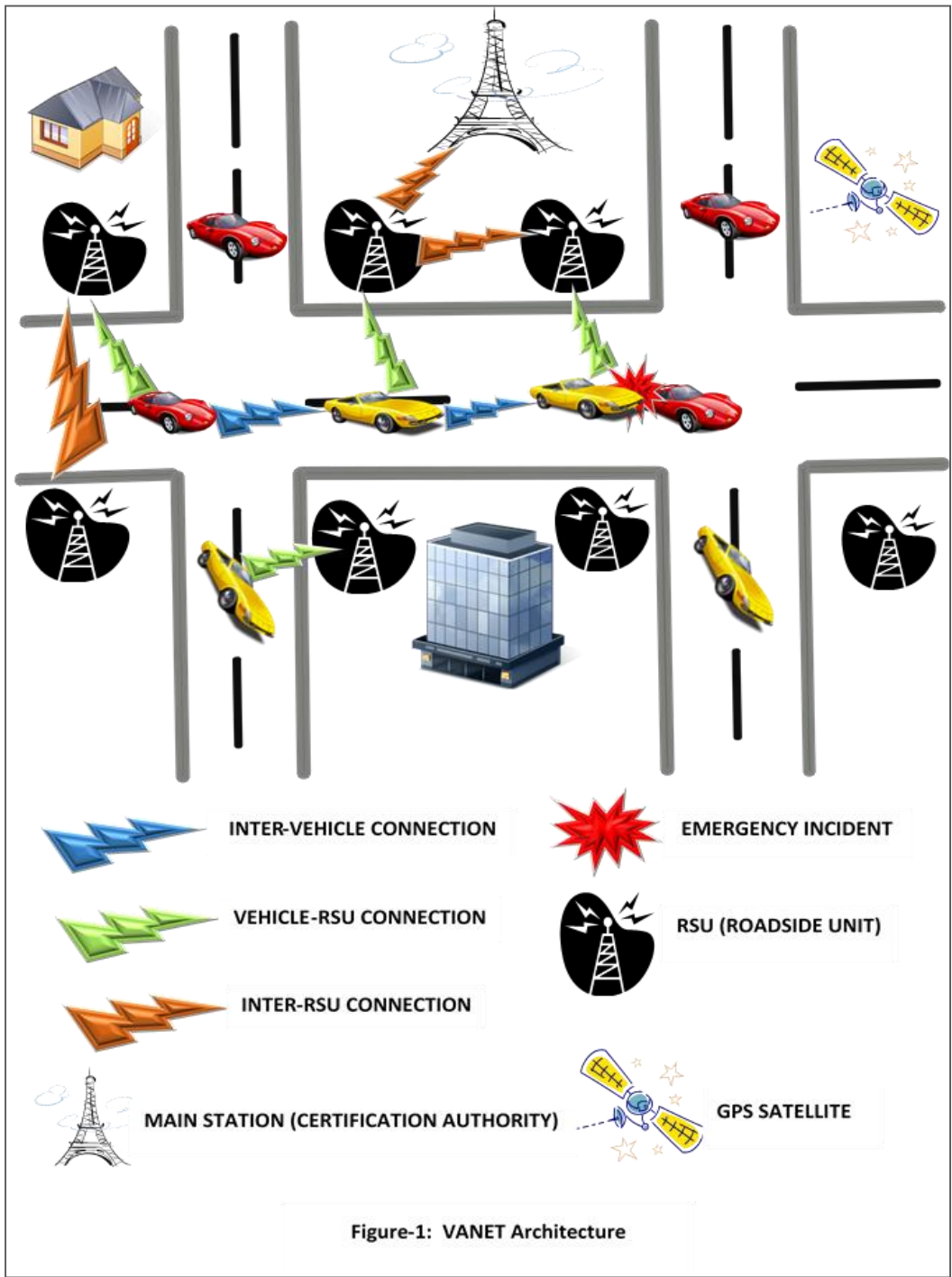
In Speed management, vehicle's driver govern vehicle's speed and driving is attained easily with eviction of useless stoppages. Regulative/contingent speed limit warning, green light optimum speed advisory are illustrations of speed management.

- **Co-operative Navigation**

In Co-operative navigation throughput of traffic is improved by co-operative navigation among vehicles or vehicles/RSU. Eviction of traffic jam through Self-Organising Traffic Information System (SOTIS), hazardous location warning, approaching vehicle warning and many more are illustrations of co-operative navigation.

## 3. **Advertorial and Commercial Applications**

Advertorial and Commercial Applications are determined towards offering entertainment associated messages like location of nearest shopping mall, cinema and many more. Co-operative Local Applications and Global Internet Applications are associated with Advertorial/Commercial Applications.



VANET architecture incorporates vehicles associated with On-Board Unit (OBU), RSU and Certification Authority (CA) disposed along Highways, GPS satellites, various kinds of communication between vehicles, RSU and CA depicted above in Figure 1. Routing, security, reliability, Quality of Service (QOS), Internetworking and Power consumptions are numerous challenges of VANETs but security is major concern in VANET. Security is crucial concern in VANET. Numerous security threats have diminished effectiveness of



VANET, human lives and traffic management applications. Sybil Attacks belongs to those threats diminishing effectiveness of VANET.

In Sybil Attack evil-minded nodes known as Sybil nodes imitate multiple fraud identities of one or more vehicle at same time distorting behaviour of right-minded nodes in network vulnerable to human lives. It is termed after case study of woman recognized with disjoint character disorder and recommended in or before 2002 by Brian Zill at Microsoft Research [4]. Different strategies of finding, locating and evicting Sybil Nodes in VANET are suggested and differentiated along with their flaws and strength in later sections.

## Chapter 2

# REVIEW OF LITERATURE

---

Sybil Attack was first depicted by Doucer in [4]. Different strategies for finding, locating and evicting Sybil Nodes and Sybil Attack have been proposed till now. Exerting Resource Testing [4] was fundamental direct validation strategy grounded on premise that proportion of enumerating resources like computation, storage and communication for each vehicle on network are minimal. In this strategy, verifier disseminates request instructing definite proportion of resource expenditure to acknowledge and manage vehicles that acknowledged back in given time interval. Evil-minded vehicles are furnished with numerous symmetric and asymmetric cryptographic strategies integrated tools. So, this strategy is impractical.

Newsome et al. [5] suggested Radio Resource Testing strategy grounded on premise that each vehicle has only one radio vulnerable to concurrent transmission or reception on more than one channel. Intruder may exert different vehicles for transmission to multiple radio channels. This strategy is beneficial grounded on premise that intruder cannot exert one vehicle for transmission to multiple radio channels concurrently.

Doucer [4] suggested Rationalized Trusted Certification strategy which employs Certification Authority (CA) subjected to ensure claimed identity of vehicle is authorized with assistance of Access Control List (ACL) and further circulate certificates to right-minded vehicles for communication. Vehicles identities are certified formerly connecting to network. CA are subjected to ensure preservation of certification list and one-to-one relationship between vehicles and identities. This strategy is inadequate in case of single point attack, potential congestion, scaling and dissemination cost.

Demirbas and Song [6] suggested Received Signal Strength Indicator (RSSI) strategy consequence of dissemination power exerts receiver to collaborate RSSI of message with sender-id integrated in message without hampering network with symmetric and asymmetric keys. Receiver recognizes Sybil attack upon receiving another message with same RSSI but different sender-id. Sybil node may disseminate message

with different ID's employing fluctuating dissemination power to deceive receiver. This strategy is inadequate due to erratic, time fluctuating and non-isotropic nature of RSSI.

Different strategies are grounded on Public Key Infrastructure (PKI) suggested by Raya and Hubaux [7] exerting CA to validate each vehicle with distinct public key and certificates organized by CA. Classical PKI grounded certificates employed only key information without any consideration to vehicles distinct physical knowledge provoking it defenceless to stolen authorized key pair and certificates utilized by malicious vehicle. Later Multifactor authentication strategy was suggested which exerts certificates to associate key pair information, radio coverage, transmitter coverage and so on as accomplished by CA. VANET is divided into zones. Each zone has one CA. CA of different zones oversee circulated certificates by disseminating with each other along certified channel as messages with authorized certificates are considered. In VANET, validating PKI for each vehicle at same time with different manufacturer, policies and countries or Vehicular Public Key Infrastructure (VPKI) including key dissemination and certificate administration incorporating circulation, preservation, revocation and elicitation of certificates possess prolong duration and memory. VPKI is inadequate to preserve privacy. Certificates should be changed from time to time for preserving privacy.

Guette and Bryce [8] suggested tamper proof hardware grounded strategy associated with cryptographic principles fabricated on Trusted Platform Module (TPM) integrated in vehicle. TPM certificates are certified by vehicle manufacturer and confidential information and protocols are preserved in Tamper proof hardware where replication and fabrication is impossible. So, dissemination between TPMs of vehicles are shielded from Sybil attack. TPM is enhanced alteration of certificates but CAs are significant for administration of individual vehicles. This strategy is inadequate due to flaws of tamper proof hardware suggested by Anderson and Kuhn in [10]. Evil-Mined vehicles with exploitation of semiconductor test device can invade chip-sized tamper resistance hardware for fetching certificates components by inspection and utilization of chip's components.

Eschenauer and Gligor [11] suggested Random Key Pre-distribution strategy employing each vehicle with arbitrary group of keys from huge key space prior to concur on distinct key or shared secret key between two different arbitrary groups of keys of two different vehicles for communication.

Chan, Perrig and Song [9] suggested q-composite random key pre-distribution strategy grounded on above explained strategy which employs q-distinct keys ( $q \geq 1$ ) instead of single key for reliable communication between two vehicles. This strategy certifies the key and integrates identity of vehicle with key circulated to vehicle. Sybil nodes will fail at key certification test due to irrelevant equivalence with compromised key set. This strategy is inadequate to preserve privacy due to association of vehicle's identity along keys, communication overhead when two vehicles are not straight associated and computational overhead.

Park, Aslam, Turgut and Zou [12] suggested Timestamp series strategy grounded on Roadside Unit Support (RSU) employs RSU incorporating certified timestamps to circulate certified Timestamps associated with vehicles self-initiated public key to each vehicle after moving along RSU. It is infrequent for arbitrary two or more than two vehicles to move along slightly numerous RSUs repeatedly at same time. Sybil attack is recognized if numerous messages disseminated by vehicles incorporates identical timestamp series. This strategy is inadequate to preserve privacy and unable to recognize Sybil attack if RSU are located at intersections and complex roadways in urban area. This strategy is unable to restrain vehicles from acquiring different timestamps from RSU. It is grounded on premise that VANET incorporates limited number of vehicles.

Zhou et al., Choudhury, Ning and Chakrabarty [13] suggested Privacy Preserving Strategy employing Department of Motor Vehicles (DMV) to circulate discrete pool of pseudonyms hashed with discrete value to vehicles and further exerted for obscuring vehicles distinct identity. Pseudonyms are exerted for disseminating traffic messages instead of vehicles real identities for privacy. Hashing restrains malicious vehicle from exploitation of pseudonyms. Hashed Values are preserved at RSU and DMV. Co-ordination of RSU and DMV association can recognize any deceptive pseudonym. Minimal knowledge about vehicles at RSU provokes it to transmit all deceptive pseudonyms upon intuition along with hashed value to DMV which further validates pseudonyms preliminary circulated to vehicles. This strategy preserves privacy but inadequate to mitigate false alarm over transmission of each deceptive pseudonym to DMV as overheads are fairly moderate which further provokes inflation in burden and time dissipation to DMV. Vehicles disseminating farther from consideration zone of RSU provokes termination of suggested strategy.

Mekliche and Moussaoui [14] suggested Location-grounded privacy preserving strategy almost identical to strategy suggested by Zhou et al., Choudhury, Ning and Chakrabarty [13] except dissimilarity that burden and false alarm on DMV is minimized due to co-ordination among nearby RSU in former strategy. Co-ordination diagnoses position of deceptive pseudonyms and further computes separable extent among position of malicious nodes. If separable extent is above threshold then RSU disseminates deceptive pseudonym to DMV for further certification where fine grained hash of deceptive pseudonym is computed for distinction among actual attack and false positive.

Zhou and Chigan [15] suggested Dynamic Trust Token (DTT) strategy for assisting node co-ordination and preserving packets during dissemination by exerting both symmetric and asymmetric cryptography and further exerting Neighbourhood Watchdog to provoke Trust Token grounded on sudden performance for certification of packet exactness. Each vehicle in DTT is exerted as Predecessor, Relay and Successor for per packet dissemination. Relay is exerted for packet dissemination. Predecessor is exerted for fabrication of trust token with assistance of Watchdog. Successor is exerted for conclusion on accepting or discarding of packet. Each dissemination of packets incorporates four phases: Packet Relaying, Behaviour Evaluation, Token Relaying and Packet Acceptance. This strategy is inadequate to trace back actual packet dispatcher after packet disseminates through numerous hops and key administration including circulation, preservation, revocation and elicitation possess prolong duration and further fabricates burden to huge unrestrained VANET.

Triki, Rekhis, Chammem and Boudriga [16] suggested RFID grounded Privacy Preserving strategy exerting two forms of validation methods. First method exerts RFID tags associated within vehicles for acquiring short span certificates from RSU after validation of vehicles along RFID tags by RSU. RFID tags and RSU are associated with Vehicle Identification Number (VIN) and RFID reader respectively. Second method exerts acquired certificates for validation to neighbours. This strategy is grounded on premise that network is split into various regions. Each region incorporates numerous RSU moreover one RSU among them is appointed as controller or Road Side Controller (RSC) for that region further associated with CA. Different regions RSCs are associated together for interchange of information analogous to circulated certificates, accumulated surveillance and investigated reports. Vehicle's certificates are renewed on transition from one region to another restraining intruders against surveillance of vehicles. Exertion

of RSU at road intersections may sanction vehicles to acquire numerous authorized certificates. During certificates revocation, precise and immediate recognition of vehicle is essential to restrain them from acquiring numerous identities from same RSU. False negatives analogous to vehicles disseminating farther from consideration region of RSU are minimized with assistance of observers associated within vehicles, RSU and RSC. Burden on RSU is minimized due to allocation of observers associated within vehicles, RSU and RSC. Observers are exerted for accumulation, substitution and evaluation of data analogous to volatile circumstances. This strategy preserves privacy as VIN associated within RFID tag is never disseminated inside VANET. Exerting RFID systems [17] is convenient interpretation regarding vehicles recognition and localization.

Eun-Kyu Lee, Sungwon Yang, Soon Y. Oh, and Mario Gerla [17] suggested RF-GPS(RFID supported GPS systems) enhancing GPS position preciseness by utilizing approaches like RF-GPS and DGPS for recognition and localization of vehicles with cooperation of mobile referral nodes on network. It sanctions Non-GPS vehicles to estimate their location and travel information via RFID and IEEE 802.11 radio respectively by notifying GPS implemented neighbour vehicles. Vehicles interchange data among themselves using mobile RFID reader/tag set. RSU incorporates RFID reader exerted for certifying VIN from RFID tags associated within vehicles. Fragment of vehicles incorporates GPS systems but RFID reader/tag set is incorporated by all vehicles.

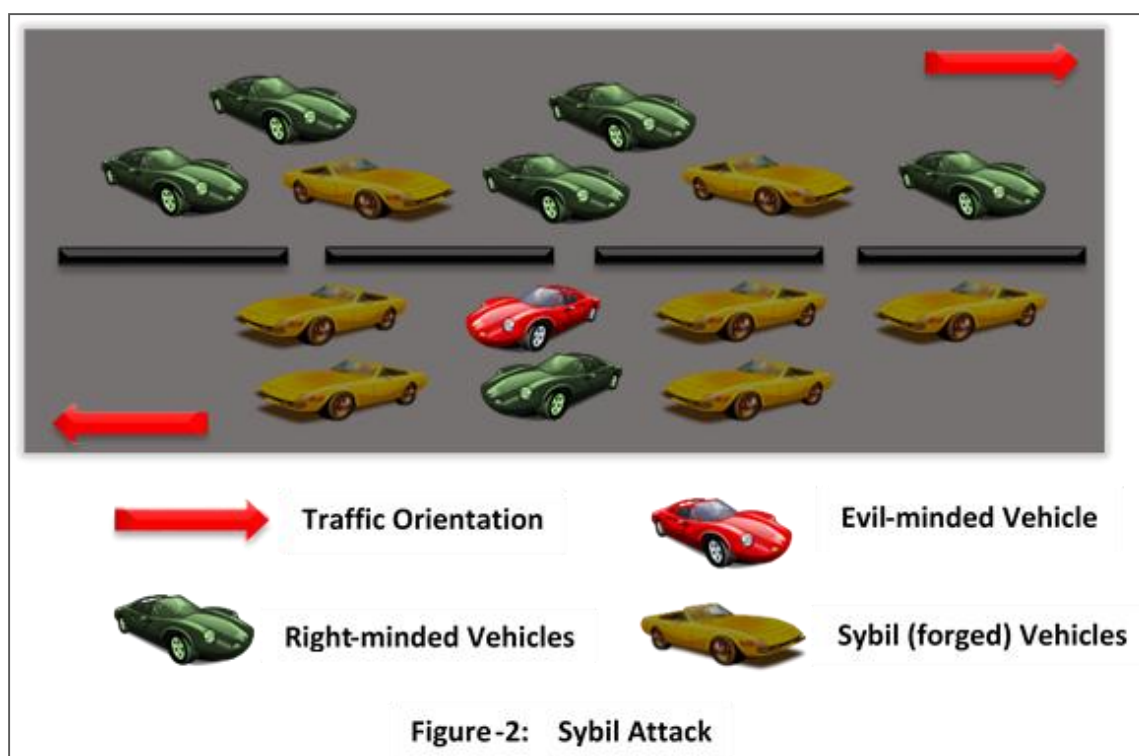
# Chapter 3

## PRESENT WORK

### 3.1 PROBLEM FORMULATION

#### 3.1.1 Principal emphasis

Principal emphasis of this study is recognition and eviction of Sybil attack in VANET. Sybil attack is security concern in VANET which diminish effectiveness of VANET, human lives and traffic management applications. In Sybil Attack evil-minded nodes known as Sybil nodes imitate multiple fraud identities of one or more vehicle at same time in peer-to-peer network distorting behaviour of right-minded nodes in network vulnerable to human lives as depicted under in Figure 2.

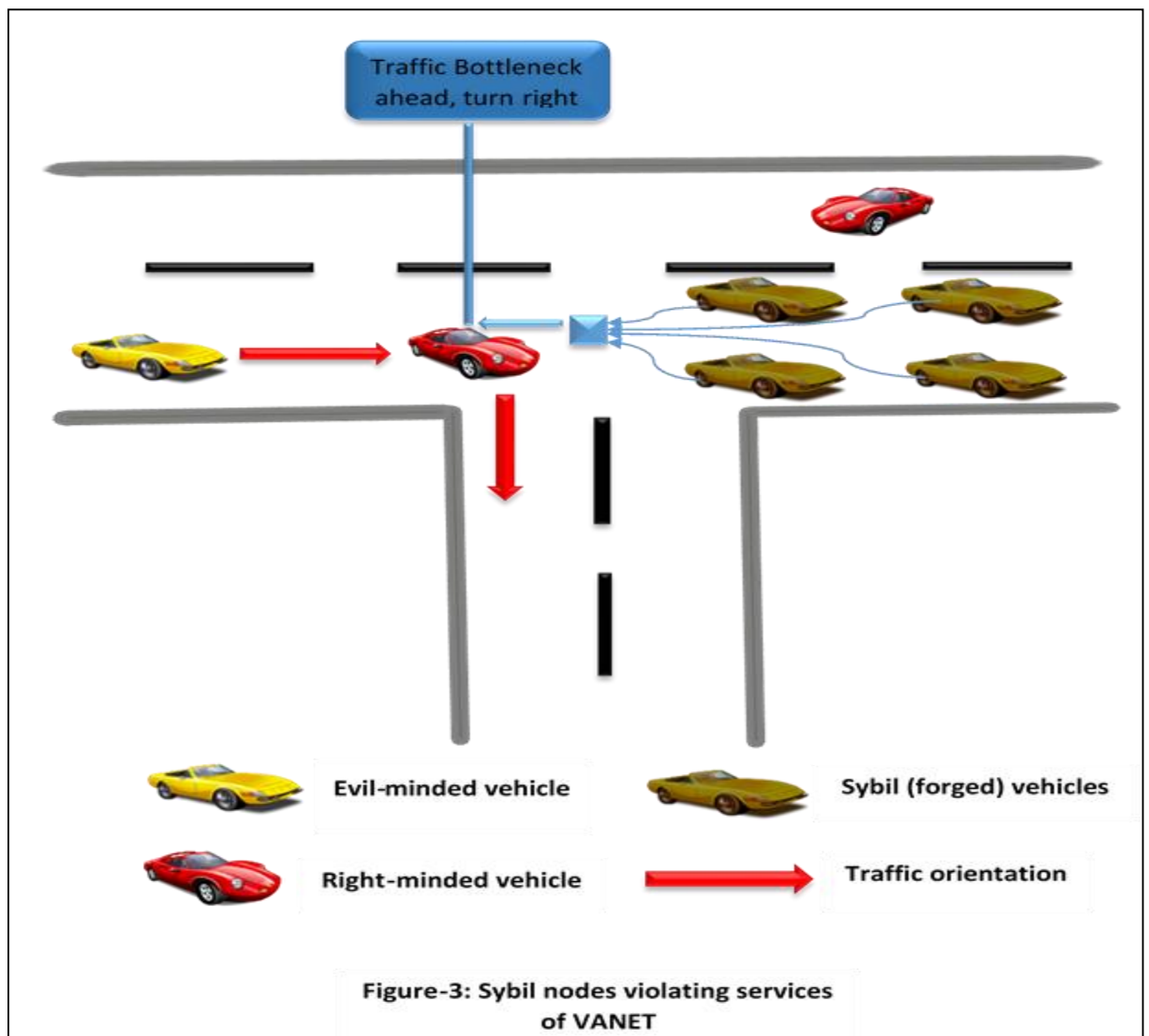


#### 3.1.2 What is Sybil Attack?

In Sybil attack, evil-minded vehicle can forge his identity as every vehicle has key pair and evil-minded vehicle may misappropriate other vehicle with his own key pair. Evil-minded vehicle can forge identities of other vehicles by theft of key pair of right-minded

vehicle and misappropriate that key pair by representing other vehicles with stolen key pair.

Absence of centralized trusted authority and presence of distributed operation in peer to peer network in VANET provokes fabrication of multiple fraud identities of one vehicle at same time in network. Entities are proclaimed in peer-to-peer network with assistance of identities and mapping of identities to entities is many-to-one. In peer-to-peer network, replication is exerted for protection against loss of integrity, privacy but evil-minded evade this feature of peer-to-peer network which further disrupts integrity and privacy. Multiple identities in VANET are exerted for adequacies like reliable data dissemination, reliable traffic administration for prevention of collisions, resource sharing and integrity but evil-minded nodes evade these adequacies either for personal benefits or for fun as depicted below in figure 3.





In above depicted figure, Sybil nodes disseminate erroneous message to right-minded nodes for their personal benefits which further violates services of VANET.

Vehicles in VANET are recognized by certificates associated with public/private key pair. Evil-minded nodes may proclaim multiple distinct identities in VANET by theft or misappropriation of certificates and public/private key pair of right-minded nodes with assistance of numerous passive and active attacks like eavesdropping, masquerading, traffic analysis etc.

### **3.1.3 Issues due to Sybil Attack**

Actions accomplished by evil-minded nodes in VANET as examined above provokes numerous issues in VANET which diminish effectiveness of VANET applications concerning traffic administration, human lives, reliable data dissemination, entertainment etc. Various issues occurring in VANET due to Sybil attack and issues in formerly fabricated techniques are stated below:

- Recognition and eviction of evil-minded nodes or Sybil nodes or Sybil attack in VANET.
- Classification of recognized nodes to honest or deceptive premised on disseminated data.
- Classification of recognized data to faulty or correct.
- Recognition of person's identity driving particular vehicle.
- Authenticity of vehicle's identity captured by numerous automatic identification and data capture (AIDC) techniques.

### **3.2 OBJECTIVES OF STUDY**

Objectives of this study is resolution of numerous issues encountered in VANET due to Sybil attack, as stated under:

- Recognition and eviction of evil-minded nodes or Sybil nodes or Sybil attack in VANET.
- Classification of recognized nodes to honest or deceptive premised on disseminated data.
- Classification of recognized data to faulty or correct.
- Recognition of person's identity driving particular vehicle.

- Authenticity of vehicle's identity captured by numerous automatic identification and data capture (AIDC) techniques.

Other objectives of this study are discussed under:

- Provision of VANETs services and applications to vehicles in network without any issues and revocation of certificates from violating vehicle.
- Safe recognition of vehicles through RFID and eviction of vehicles from VANET services who violate services of VANET and refrain other vehicles in VANET from acquisition of services with injection of faulty data in network.
- Safely recognition of evil-minded vehicles with association of RFID and single allocated certificate. Certificates for each vehicle are governed by Certification Authority (CA).
- Classification of disseminated data in network as faulty or correct with assistance of voting algorithm in each sub-network separately which further assist in classification of vehicles to honest and deceptive.
- No allocation of different certificates to same vehicle on adaptation from one zone to other. Single certificate make it easy to recognize violating vehicle without any consumption of extra storage space for certificates.
- Integrity & authenticity of disseminated data with associated assistance of digital signature and watchdog.

### **3.3 RESEARCH METHODOLOGY**

Research methodology is detailed and step-by-step description of proposed strategy for satisfying numerous objectives of study. It is description of each step necessitated in proposed strategy for recognition and eviction of Sybil Attack in VANET and satisfying numerous objectives of this strategy further persuading it as cost-effective strategy for recognition and eviction of Sybil Arrack in VANET.

#### **3.3.1 Principal elements**

Principal elements of proposed strategy persuading it as cost-effective strategy in terminology of diminished spatial, temporal and complexity overhead are:

- **RFID**  
RFID is AIDC technique exerted for automatic identification of vehicles with assistance of RFID tags/reader. Vehicles penetrating in proximity of RFID readers

associated on roadside are automatically identified by RFID reader with assistance of RFID tags associated within vehicles accumulating vehicle's information. RFID tags associated within vehicles includes information like VIN, chassis number etc. preserved beyond encryption codes which further persuades only certified RFID readers to access RFID tags.

- **Voting Algorithm**

Voting algorithm is exerted in cluster of vehicles per sub-network for classification of vehicles to be honest or deceptive. All vehicles per sub-network disseminate their trust value of particular vehicle to CA. Threshold of trust value is set and vehicles having trust value beyond threshold value are classified as deceptive. Classified information is disseminated to other sub-network by CA to CA dissemination. Vehicles associated within one sub-network cannot disseminate with vehicles associated within other sub-network directly. CA can disseminate with other CA and vehicles associated within his sub-network but cannot disseminate with vehicles of other sub-network. It can be exerted in association with Watchdog for improved classification of vehicles.

- **Watchdog**

Watchdog is exerted in association with voting algorithm and digital signature for classification of both vehicles as honest or deceptive and data as correct or faulty. Initiating vehicle disseminating data within network through intermediate vehicles should be trustworthy. Each vehicle is provisioned with watchdog element. When any vehicle disseminate data to intermediate vehicle than disseminating vehicle eavesdrop on behaviour of intermediate vehicle. If intermediate vehicle drops data or alter data or does not disseminate data to other vehicles within particular threshold value than that intermediate vehicle is classified as deceptive and that information is disseminated to other vehicles associated within network.

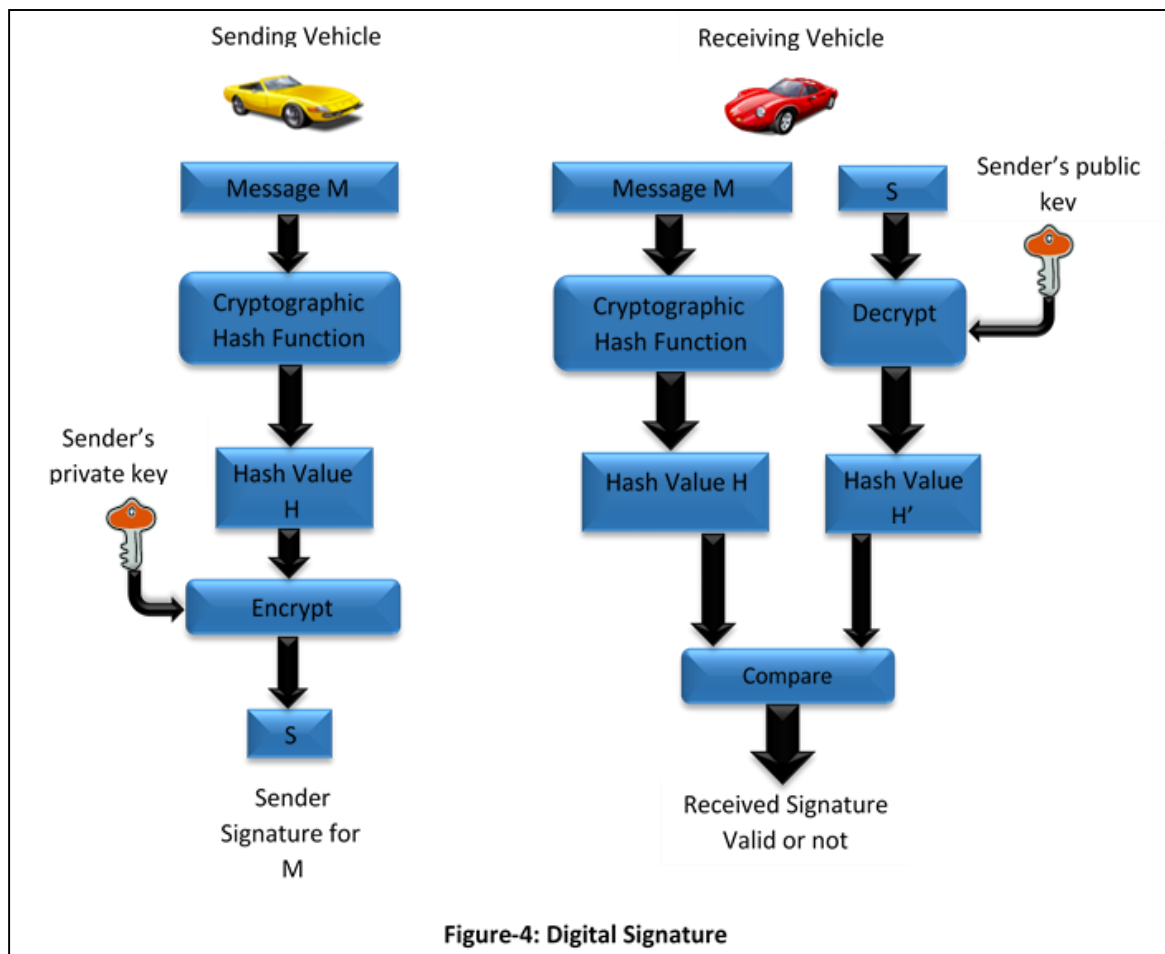
- **Digital Signature**

Digital signature (Asymmetric cryptography) is exerted in association with watchdog for integrity and authenticity of disseminated data and classification of disseminated data as faulty or correct as depicted below in figure 4. Cryptographic

hash function for hashing is exerted in fabrication of digital signature. As hashing has one-way and collision free property which means any alteration to disseminated data will be easily recognized.

- **Single Certificate**

Vehicles penetrating in proximity of VANET are allocated with single lifetime certificate per vehicle. It is exerted in association with RFID and can be in association with any of above described elements. Single allocated certificate diminish spatial, temporal and complexity overhead. Through single certificate vehicles violating services and applications of VANET are easily recognized and evicted by certificate revocation. Unlike other strategies described in Section 2, if vehicles are forced to change certificate on adaptation from one zone to other than evil-minded vehicle will violate the network with different certificates of different zone which further increases spatial, temporal and complexity overhead.



Important points to be considered for proposed strategy are described below:

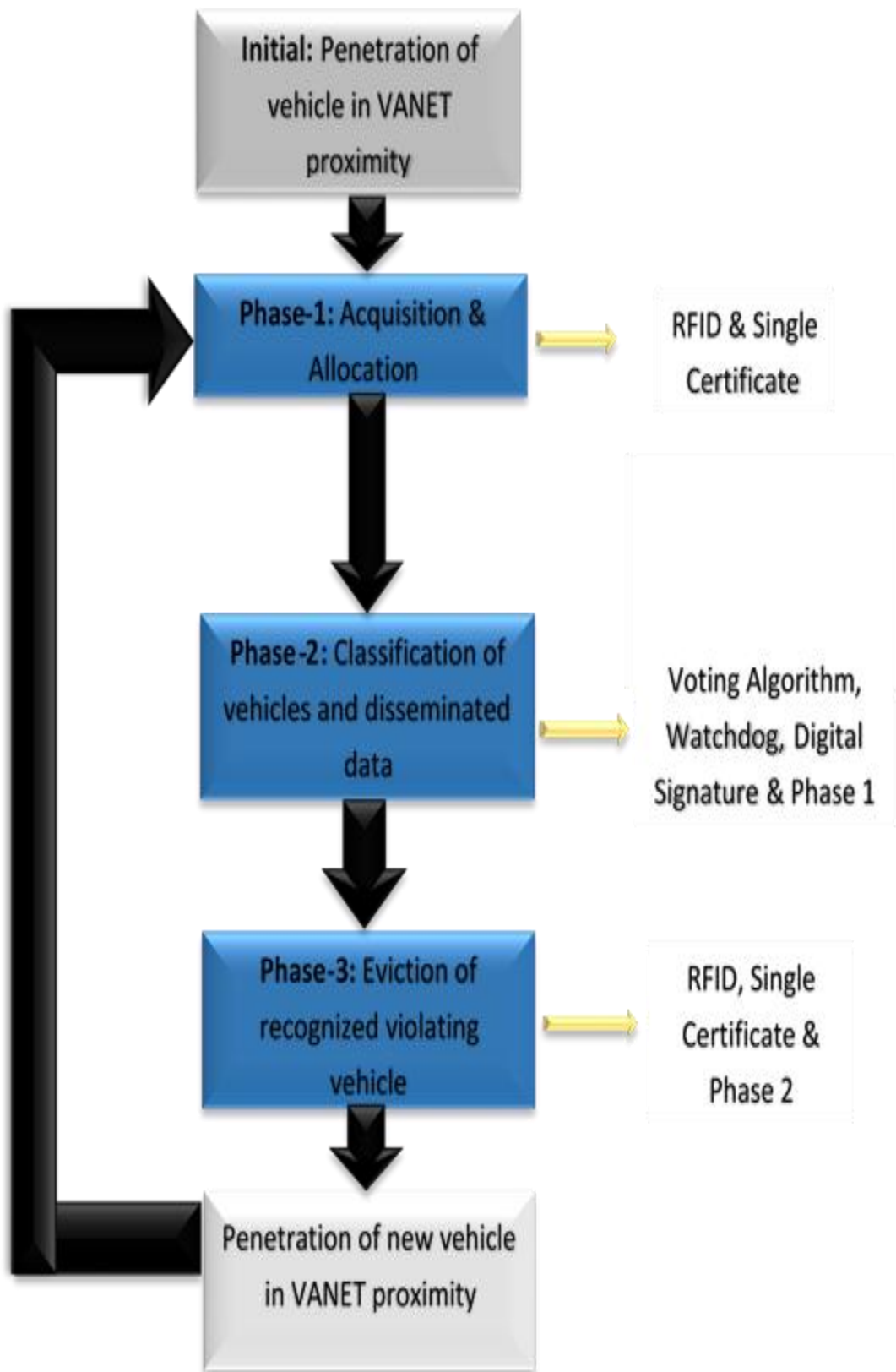
- Each VANET is split into several sub-networks.
- Each sub-network has one CA.
- All Vehicles in single sub-network disseminate with their respective CA.
- RFID readers are positioned at every entrance point of network.
- RFID tags are associated in each vehicle penetrating in proximity of network.
- Dissemination within sub-network occurs in CDMA to avoid interference among two or more different sub-networks.
- Dissemination of CA with CA of other sub-networks for circulation of allocated certificates to vehicles.
- Initial vehicle in network disseminating data should be trustworthy.
- Data captured through RFID along with allocated certificates to vehicles are preserved in DMV (Department of Motor Vehicles).
- Dissemination of DMV with certified CA only.
- Dissemination of CA with DMV for mapping of certificate with captured RFID data of particular vehicle.

### **3.3.2 Phases of proposed strategy**

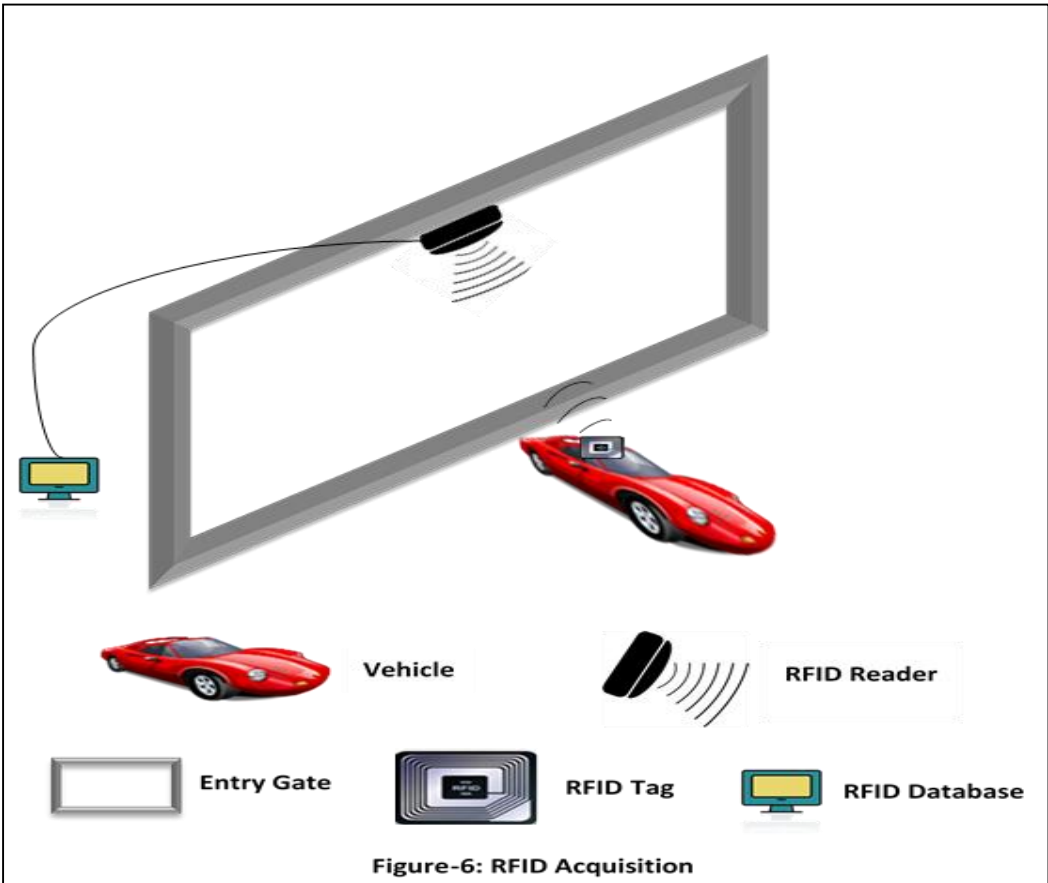
Proposed strategy along with above discussed principal elements and important points is split into 3 phases as discussed below and depicted below in figure-5:

#### **1. Phase 1 (Acquisition & Allocation)**

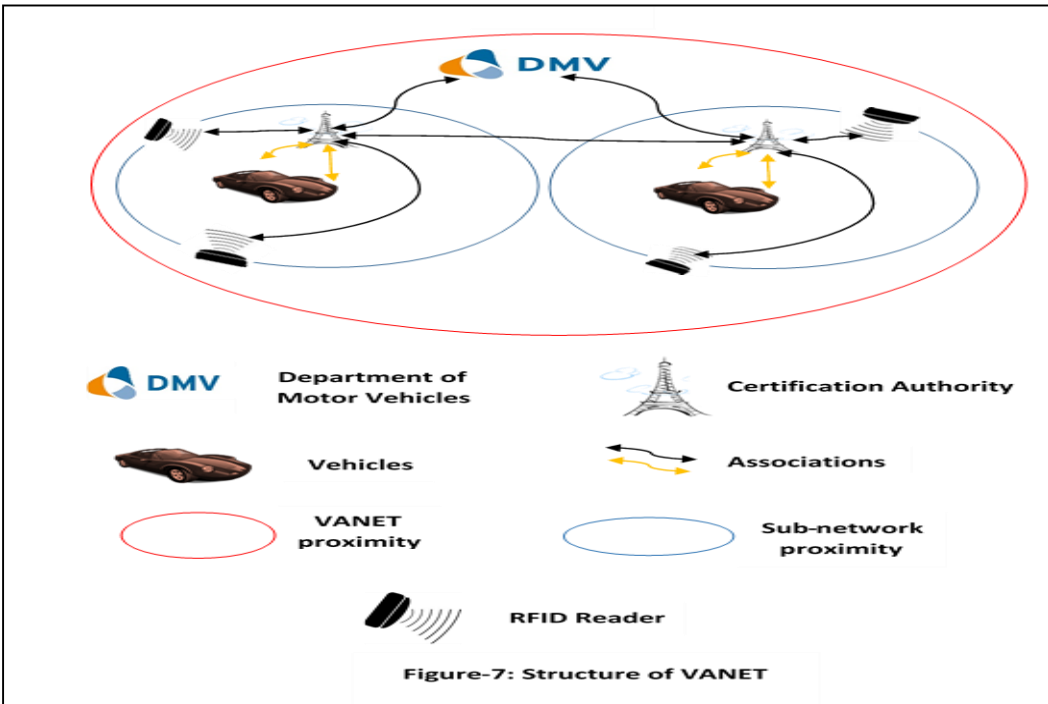
When any vehicle penetrates in proximity of VANET for first time, RFID reader positioned at initial point of network acquire information of vehicle through RFID tags associated in vehicle and CA positioned at initial sub-network allocates certificate to vehicle as depicted below in figure 6. Scanning through RFID reader and allocation of certificate for one vehicle is accomplished in consecutive order for one-to-one mapping. One-to-one mapping of RFID reader acquired data and single allocated certificate is preserved at DMV. Scanning and allocation of certificates for more than one vehicle are not accomplished in consecutive order without any duration. Little duration exist among more than one vehicle for initiation of phase 1 for prevention against reader collision.

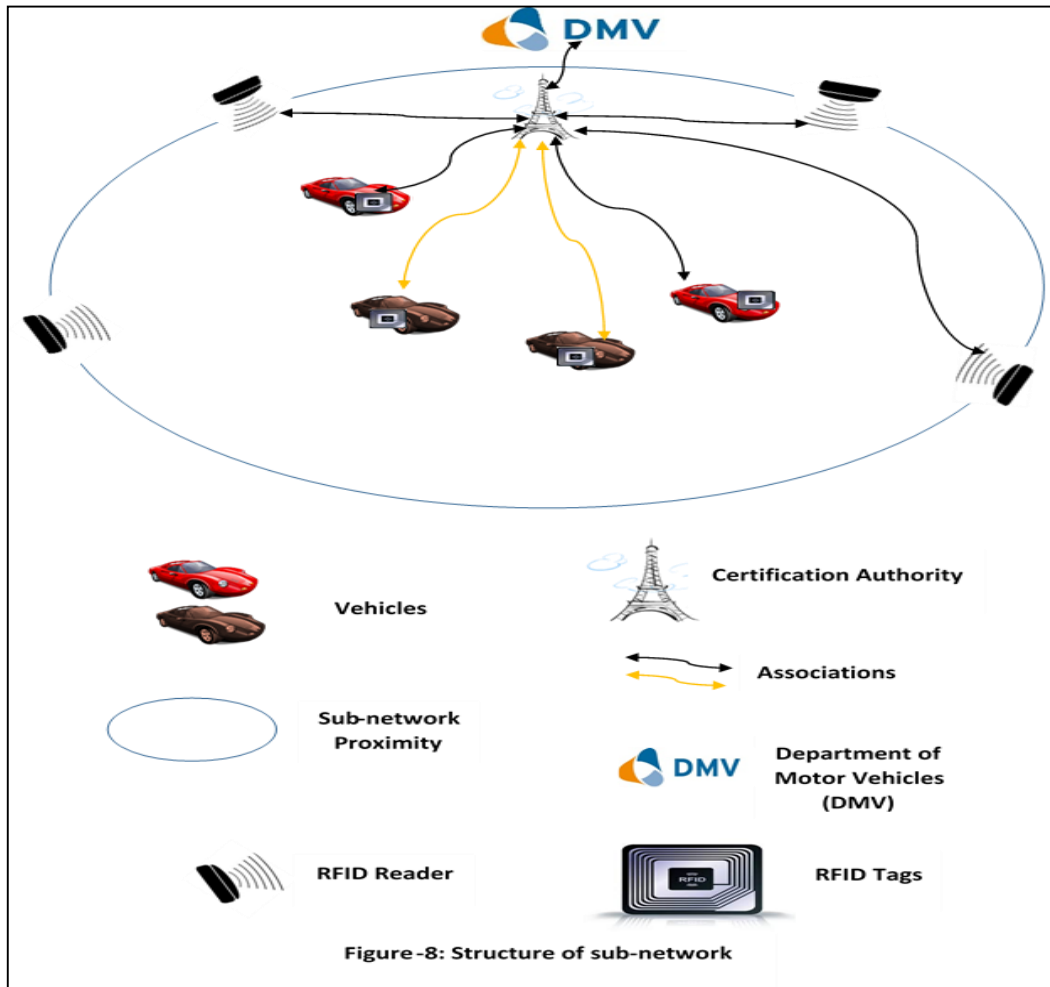


**Figure-5: Flowchart of various phases of proposed strategy**



**2. Phase 2 (Classification of vehicles and disseminated data)**





In phase 2, three prior discussed principal elements voting algorithm, watchdog and digital signature are exerted. Classification of vehicles and disseminated data is accomplished simultaneously for more preciseness. Vehicles and disseminated data are classified simultaneously as vehicles after penetrating in network disseminate data in network so classification of both vehicle and data is significant for preciseness.

Disseminated data is classified with prior discussed principal element digital signature. Sending vehicle disseminate data in digital signature manner as depicted above in figure-4 and receiving vehicle validates data by comparing hash value. If received hash value and computed hash value is same than data is unaltered and authentic else received data is altered and unauthentic. Unlike Acknowledgement grounded approaches exerted in MANET for eviction of Sybil attack cannot be exerted in VANET due to high mobility in VANET. So digital signature is exerted as sender disseminates data with computed digital signature and after that it is job of receiver to validate received data.



Vehicles are classified with prior discussed principal elements voting algorithm and watchdog. In voting algorithm range of threshold value is prescribed from -3 to +3 for each vehicle penetrating in network and initial data value for each vehicle is prescribed 0. Initial vehicles disseminating data in network should be trustworthy. It is exerted per sub-network. When any vehicle disseminates data then receiving vehicle gives positive or negative feedback for that vehicle to CA and CA to DMV. On positive feedback data value is increased by 1 and on negative feedback data value is decreased by 1. Vehicles beyond negative data value -2 are classified as deceptive. If any vehicle has data value +3 than on positive feedback it will remain +3 only to prevent any vehicle becoming deceptive afterwards and same is case of data value -3. If any vehicle has data value -3 than on negative feedback it will remain -3 only to motivate vehicle to disseminate correct data. For more clarification and preciseness CA disseminates with DMV.

Side by side vehicle disseminating data to intermediate vehicle exerts watchdog to check actions of intermediate vehicle. Network is designed in such manner that if intermediate vehicle does not disseminate data to other vehicle in threshold time of 3 than that vehicle is automatically prescribed negative feedback. Each CA preserves data value for each vehicles located within their sub-network proximity.

### **3. Phase 3 (Eviction of recognized violating vehicle)**

In phase 3, two prior discussed principal elements RFID and Single certificate are exerted grounded on outcomes acquired from prior phase (Phase 2) for formation of useful conclusions. When data value of any vehicle acquired from phase 2 beyond -3 than that vehicle is classified as deceptive and CA broadcast this information to vehicles within its proximity and also to adjoining CA. These adjoining CA broadcast same information within their proximity. These CA also reports about violating vehicle to DMV by informing them vehicle private/public key pair. Now, DMV acquires associated RFID data with key pair from their database and evict vehicle from network by revocation of vehicles certificate. If violation is more hazardous than DMV catch person driving that vehicle through associated RFID data. RFID accumulates VIN number and through VIN number owner of particular vehicle can be easily recognized and penalized.

## Chapter 4

# RESULTS AND DISCUSSION

---

Strategy proposed in preceding chapter for recognition and eviction of Sybil attack in VANET is implemented in NS-2 (Network Simulator 2) version 2.35 integrated with NAM, XGRAPH, GAWK.

NS-2 is associated with two languages:

- TCL (Tool Command Language)
- C++

NAM is utilized for pictorial analysis of network topology. Output file produced through NAM comprises of network topology information such as nodes along with their configuration and trace data.

GAWK is utilized for analysis of trace files for estimation of numerous factors like throughput, delay, packet delivery ratio.

XGRAPH is utilized for illustration of 2D graph on X display along with input either from data files or standard input if not any data file is indicated. It is interpreted with titles, axis labels etc.

GNUPLOT can also be utilized for illustration of 2D/3D graph similar to XGRAPH.

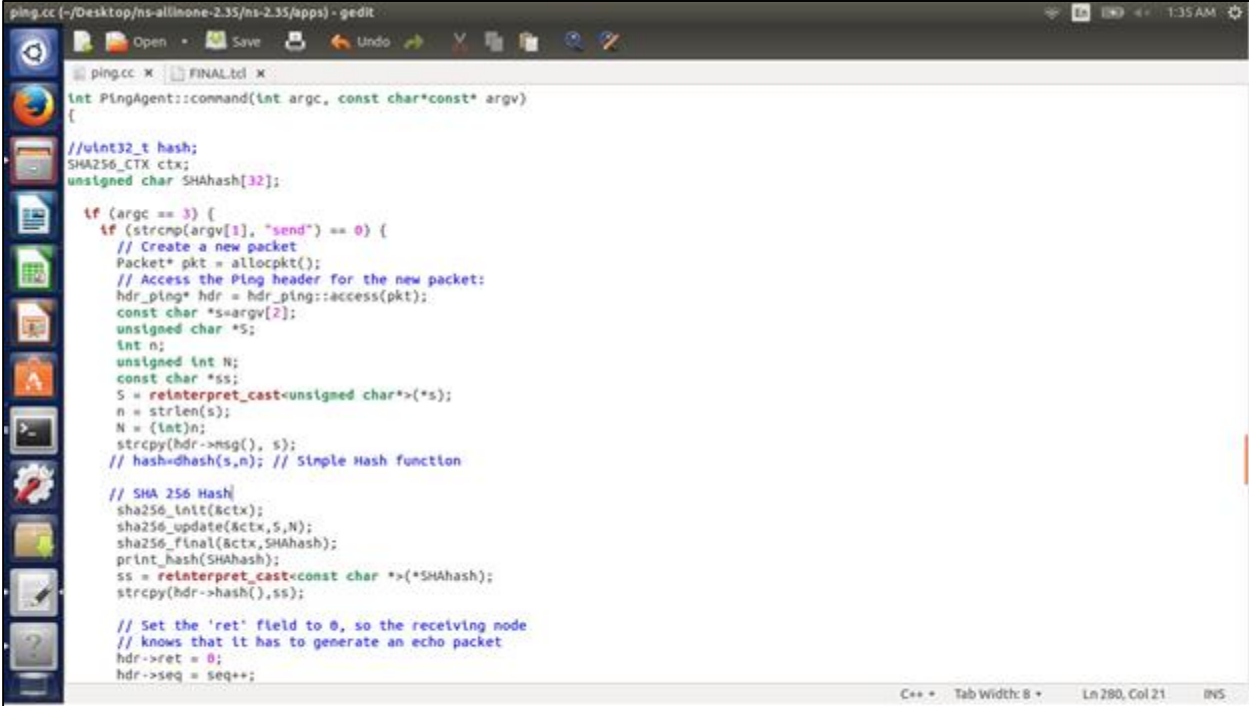
### **4.1 File formats utilized**

Files of numerous format are utilized in ns-2 for analysis such as:

- Trace Files (.tr)
- NAM Files (.nam)
- CC Files (.cc)
- TCL Files (.tcl)

## 4.2 Protocol utilized and revised

Ping protocol is utilized and revised with digital signature. [ping.cc](#) & [ping.h](#) are files revised in ns-2 for addition of digital signature as depicted below in figure 9 and figure 10.



```
ping.cc (-/Desktop/ns-allinone-2.35/ns-2.35/apps) - gedit
ping.cc x FINAL.tcl x
int PingAgent::command(int argc, const char*const* argv)
{
//uint32_t hash;
SHA256_CTX ctx;
unsigned char SHAhash[32];

if (argc == 3) {
if (strcmp(argv[1], "send") == 0) {
// Create a new packet
Packet* pkt = allocpkt();
// Access the Ping header for the new packet:
hdr_ping* hdr = hdr_ping::access(pkt);
const char *s=argv[2];
unsigned char *S;
int n;
unsigned int N;
const char *ss;
S = reinterpret_cast<unsigned char*>(s);
n = strlen(s);
N = {int}n;
strcpy(hdr->msg(), s);
// hash=dhash(s,n); // Simple Hash function

// SHA 256 Hash
sha256_init(&ctx);
sha256_update(&ctx,S,N);
sha256_final(&ctx,SHAhash);
print_hash(SHAhash);
ss = reinterpret_cast<const char *>(SHAhash);
strcpy(hdr->hash(),ss);

// Set the 'ret' field to 0, so the receiving node
// knows that it has to generate an echo packet
hdr->ret = 0;
hdr->seq = seq++;
}
}
}
C++ • Tab Width: 8 • Ln 280, Col 21 • INVS
```

**Figure 9: ping.cc**



```
ping.h (-/Desktop/ns-allinone-2.35/ns-2.35/apps) - gedit
ping.cc x FINAL.tcl x ping.h x
inline static hdr_ping* access(const Packet* p) {
return (hdr_ping*) p->access(offset_);
}
char* msg() { return (msg_); }
char* hash() { return (hash_); }
int maxmsg() { return (sizeof(msg_)); }
};
// Structure for SHA256_CTX
struct SHA256_CTX{
uchar data[64];
uint datalen;
uint bitlen[2];
uint state[8];
};
class PingAgent : public Agent {
public:
PingAgent();
int seq; // a send sequence number like in real ping
int oneway; // enable seq number and one-way delay printouts

virtual int command(int argc, const char*const* argv);
virtual void recv(Packet*, Handler*);
virtual int dhash(const char*, size_t); // Compute Hash

// SHA 256 Hash
virtual void sha256_init(SHA256_CTX*);
virtual void sha256_transform(SHA256_CTX*, uchar[]);
virtual void sha256_update(SHA256_CTX *, uchar[], uint);
virtual void sha256_final(SHA256_CTX *ctx, uchar hash[]);
virtual void print_hash(unsigned char*);
};
Saving file /home/sultan/Desktop/ns-allinone-2.35/ns-2.35/apps/ping.h...
C/C++/ObjC Header • Tab Width: 8 • Ln 114, Col 19 • INVS
```

**Figure 10: ping.h**

**SHA256** is hash function introduced in **ping.cc** protocol file.

Three function definition utilized in ping.cc for hashing along are depicted below:

- sha256\_init(&ctx)
- sha256\_update(&ctx,s,n)
- sha256\_transform(&ctx,data)
- sha256\_final(&ctx,SHAhash)

### 4.3 Other Integrations in ns-2

Apart from digital signature, RFID is also incorporated in ns-2.

Six files utilized for RFID incorporation in ns-2 are depicted below:

- **rfidPacket.cc & rfidPacket.h**
- **rfidTag.cc & rfidTag.h**
- **rfidReader.cc & rfidReader.h**

Various files needed to be revised for integration of new protocol in ns-2 are depicted below:

- **makefile** : Path of .cc & .o files of new protocol must be introduced in it and after inclusion, ns-2 necessities to recompiled.
- **ns-default.tcl** : Default values of various parameters of new packet type must be included in it.
- **Packet.h** : For visualization of new packet type in ns-2, it must be defined in it.

After recompilation of ns-2, new protocol is integrated in it.

### 4.4 NSTK

**FINAL.tcl** is tcl file utilized for simulation.

**nstk FINAL.tcl** : This command executes both ns and tk commands. Initially dialog box prompts on execution of **nstk** as depicted below in figure 11, which further ask whether animation necessities to be opened or not.

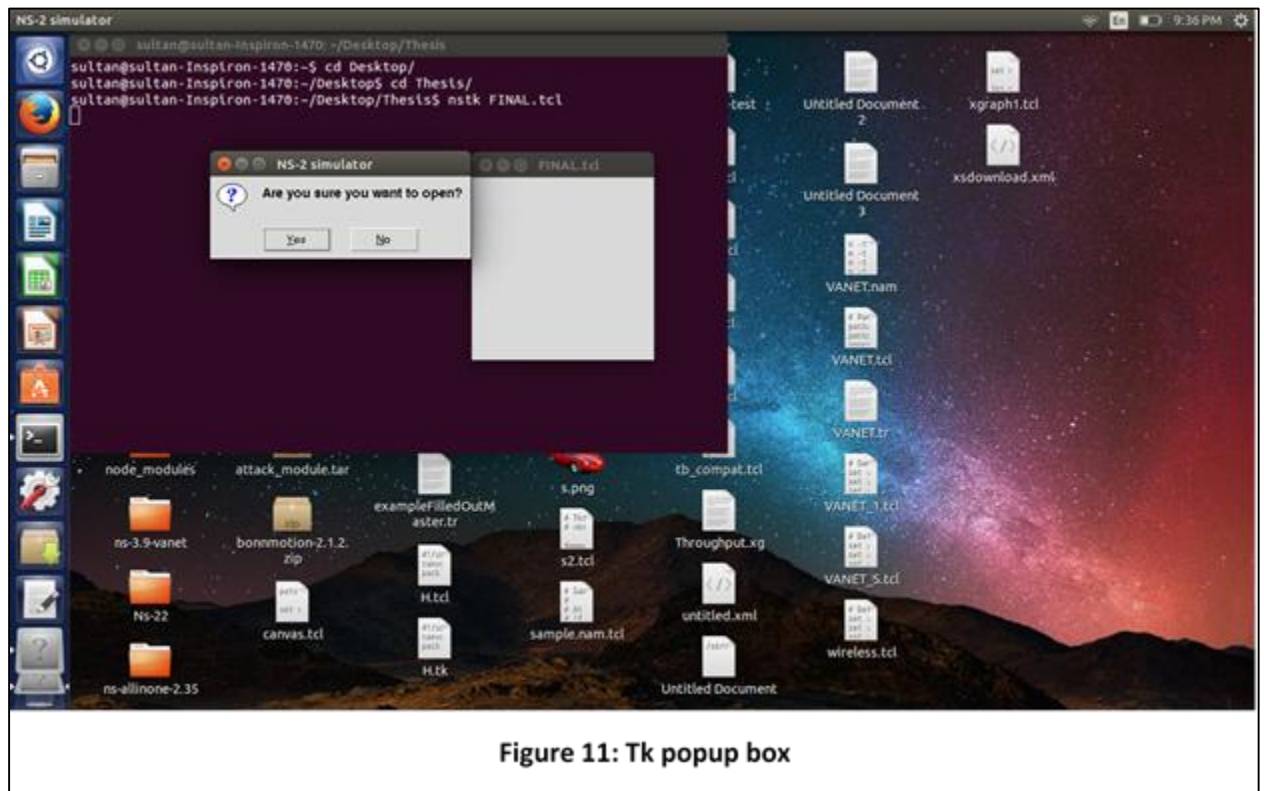


Figure 11: Tk popup box

#### 4.5 Simulation factors

- **Area:** 1600 \* 1600 m
- **Mobility Model:** Two ray ground
- **Quantity of nodes:** 8
- **Simulation interval:** 200sec
- **Routing protocol:** AODV
- **Traffic type:** Ping Agent
- **SHA 256**
- **RFID**

#### 4.6 Simulation outcomes

Various format through which simulation outcomes arise using above simulation factors are:

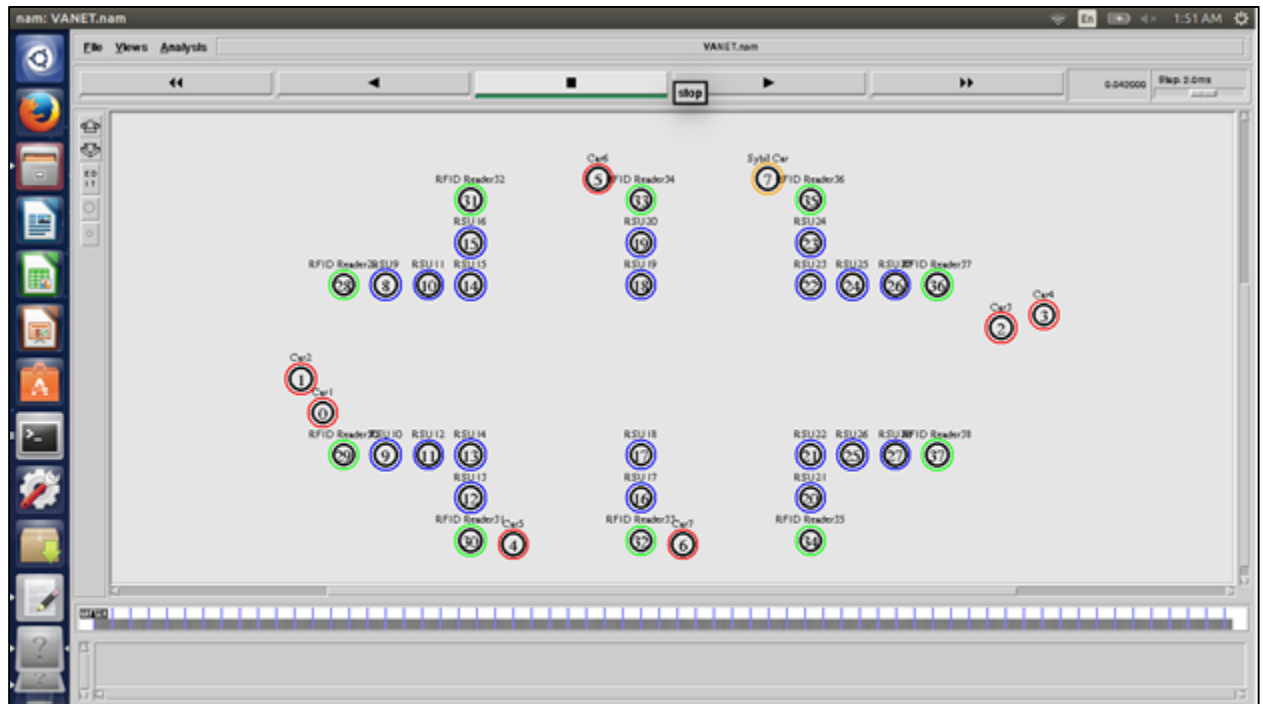
- NAM animator for visualization
- XGRAPH/GNUPLOT for graph
- AWK scripts for throughput

Outcomes of all above formats are depicted below in figures.

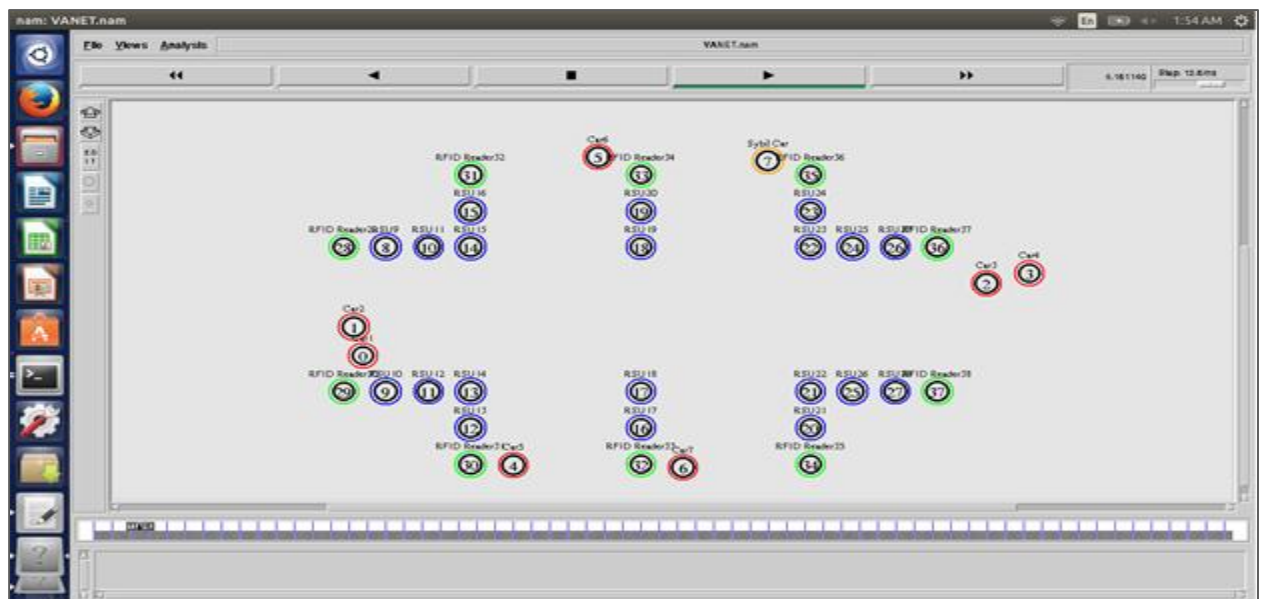
Trace annotate is also utilized for displaying messages in NAM.

Path in network topology is depicted through RSU.

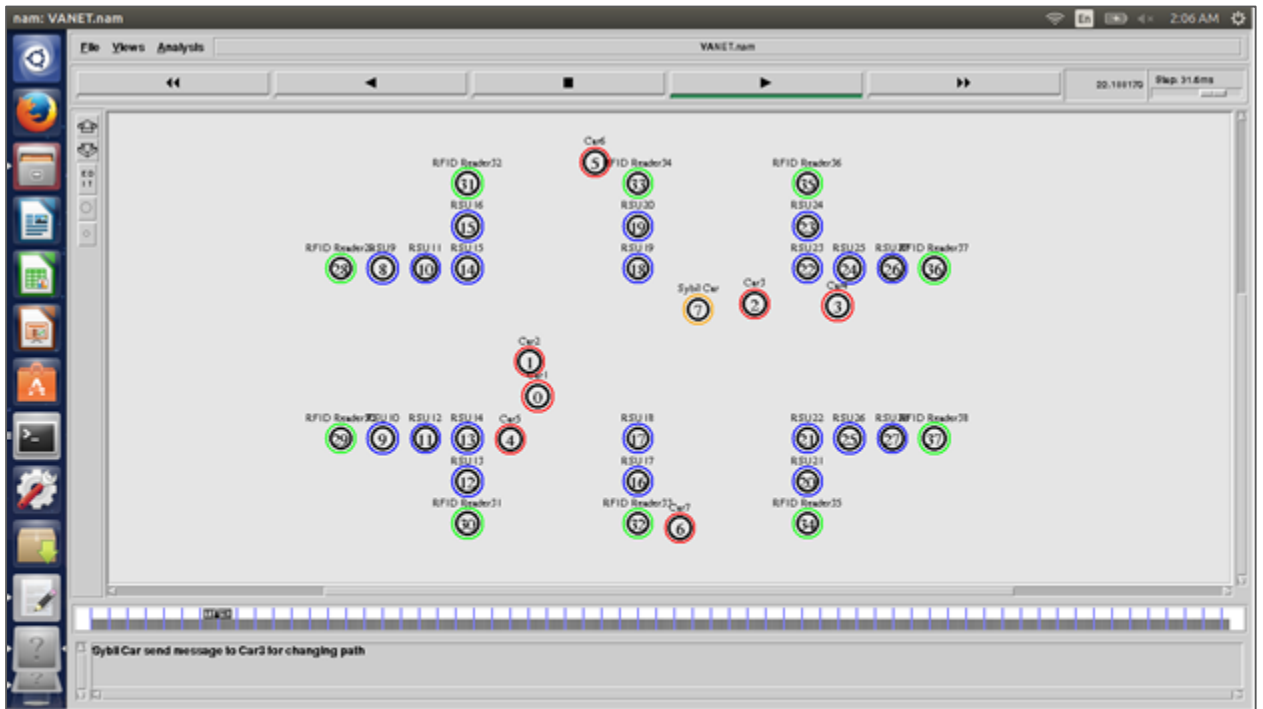
### NAM Output



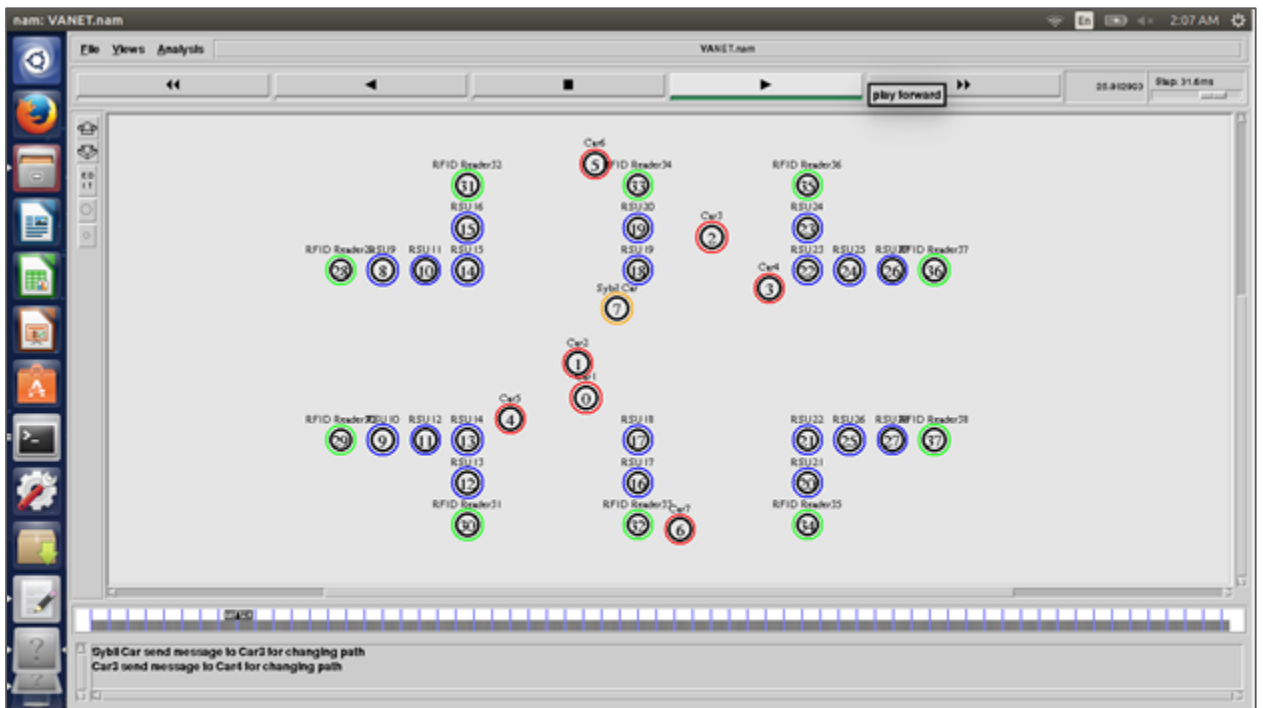
**Figure 12: Initial Network Topology**



**Figure 13: Network topology after 8.1 sec**



**Figure 14: Sybil car disseminate message**



**Figure 15: Car2 disseminate message to Car3**

## THROUGHPUT CALCULATION USING AWK

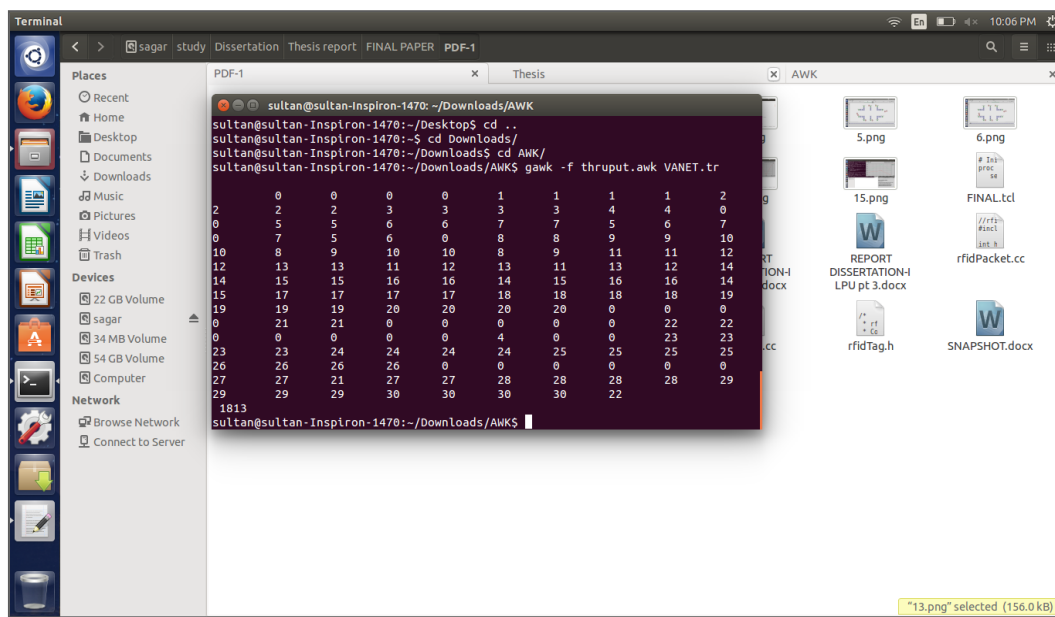


Figure 16: Throughput

## XGRAPH Output

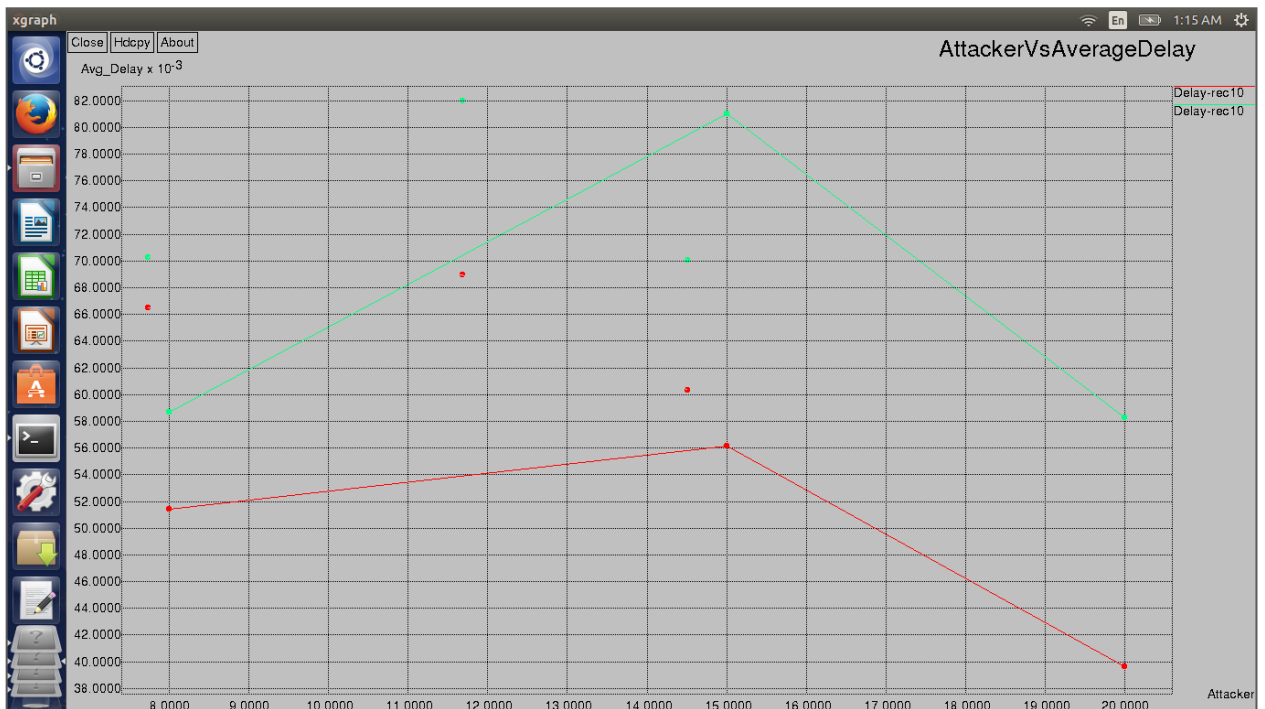
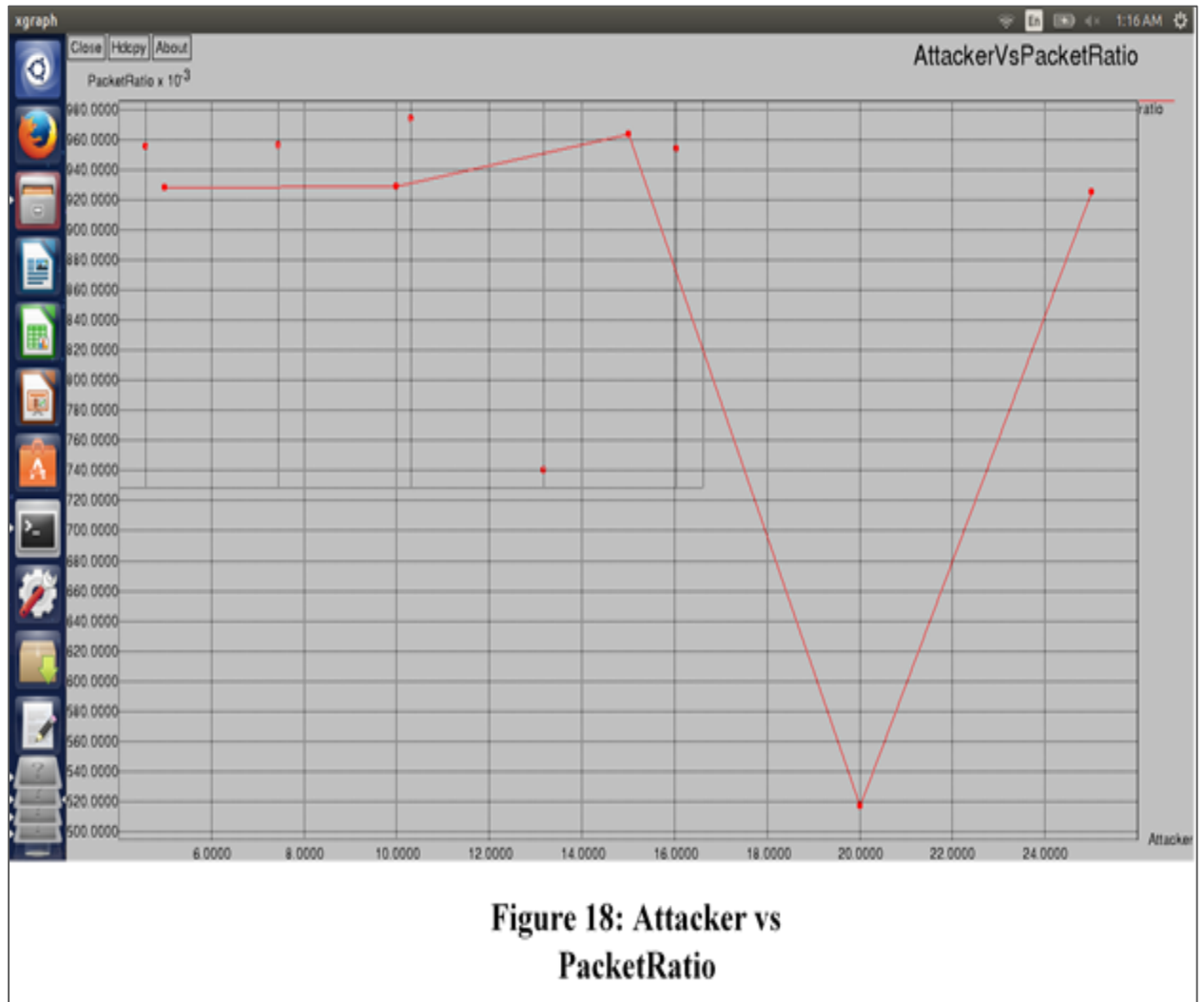


Figure 17: Attacker vs Average Delay





Graphs depicted in figure 17 and figure 18 are acquired after trace analysis. These graphs clearly depicts that proposed strategy is more effective than existing strategy. Increase in number of attackers increases average delay up to definite threshold point but after that average delay starts decreasing on increase in number of attackers and same is in case of packet ratio.

## Chapter 5

# CONCLUSION AND FUTURE WORK

---

Step-by-step description of proposed strategy described in Chapter 3 section 3.3 assist in effectual resolution of various issues described in Chapter 3 section 3.1 and objectives described in Chapter 3 section 3.2 have been effectually acquired without any trouble.

Proposed strategy has diminished spatial, temporal and complexity overhead with assistance of principal elements and whole methodology described in Chapter 5.

Proposed strategy effectively recognize and evict Sybil attack in VANET more accurately.

## LIST OF REFERENCES

---

- [1] M. Frodigh, P. Johansson, and P. Larsson. “Wireless ad hoc networking: the art of networking without a network,” *Ericsson Review*, No.4, 2000, pp. 248-263.
- [2] Joseph P. Macker, M. Scott Corson: “Mobile Ad-hoc Networks (MANET) and The IETF” Volume 2 Issue 1, January 1998, Pages 9-14.
- [3] Jun-Zhao Sun, Machine Vision & Media Process Unit, Oulu Univ, Finland: “Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”, pp. 316 - 321 vol.3, 2001
- [4] J. Douceur “The Sybil Attack” In First International Workshop on Peer- to-Peer Systems, pages 251–260, 2002.
- [5] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defences.” Proc. Of International symposium on information processing in sensor networks, pp 259–268, 2004.
- [6] Murat Demirbas, Youngwhan Song, “An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks”, In Proceedings of WoWMoM 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. 5 pp. – 570
- [7] M. Raya and J.-P. Hubaux, (2007)” Securing vehicular ad hoc networks”. *Journal of Computer Security*, 15(1), 39–68.
- [8] G. Guette and C. Bryce, “Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs),” Proc. of WISTP 08, LNCS 5019, pp. 106-116, 2008.
- [9] H. Chan, A. Perrig, and D. Song “Random key pre-distribution schemes for sensor networks”. In IEEE Symposium on Security and Privacy, pages 197–213, Berkeley, California, May 11-14 2003.
- [10] R. Anderson and M. Kuhn “Tamper resistance - a cautionary note” In Proceedings of the Second Usenix Workshop on Electronic Commerce, pages 1–11, November 1996.

- [11] L. Eschenauer and V. D. Gligor “A key-management scheme for distributed sensor networks”. In Proceedings of the 9<sup>th</sup> ACM conference on Computer and communications security, November 2002.
- [12] S. Park, B. Aslam, D. Turgut, Cliff C. Zou (2009)” Defense against Sybil attack in vehicular ad-hoc network based on roadside unit support”. In: MILCOM, pp. 1–7.
- [13] T. Zhou, R.R. Choudhury, P. Ning and K. Chakrabarty, “Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks,” Proc. of International Conference on MobiQuitous 2007, pp. 1-8, 2007.
- [14] Kenza Mekliche, Dr. Samira Moussaoui L-P2DSA, “Location-based privacy-preserving detection of Sybil attacks,” Programming and Systems (ISPS), 2013 11th International Symposium on Digital Object Identifier: 10.1109/ISPS.2013.6581485 Publication Year: 2013, Page(s): 187-192
- [15] Zhou Wang, Chunxiao Chigan, “Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs” Communications, 2007. ICC '07. IEEE International Conference on Digital Object Identifier: 10.1109/ICC.2007.652 Publication Year: 2007, Page(s): 3959 - 3964
- [16] Bayrem Triki, Slim Rekhis, Mhamed Chammem, and Nouredine Boudriga, “A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Networks” Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP, Digital Object Identifier: 10.1109/WMNC.2013.6549051 Publication Year: 2013 , Page(s): 1 - 8
- [17] LEE, E.-K., YANG, S., OH, S. Y., AND GERLA, M “RF-GPS: RFID assisted localization in vanets” Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on (October 2009).
- [18] P. Basu, N. Khan and T. D. C. Little, “A mobility based metric for clustering in mobile ad hoc networks,” in Proc. Int. Conf. Distributed Computing Systems Workshop, pp. 413-418, April 2001.
- [19] T. D. C. Little and A. Agarwal, “An information propagation scheme for VANETs,” in Proc. IEEE Intelligent Transportation Systems Conf., pp. 155-160, September 2005.

## APPENDIX

<u>ABBREVIATIONS</u>	<u>GLOSSARY</u>
AIDC	Automatic Identification and Data Capture
ACL	Access Control List
CA	Certification Authority
CAS	Collision Avoidance System
CDMA	Code Division Multiple Access
DGPS	Differentiated Global Positioning System
DMV	Department of Motor Vehicles
DOS	Denial of Service
DPP	Directional Propagation Protocol
DSRC	Dedicated Short Range Communication
DTT	Dynamic Trust Token
GPS	Global Positioning System
IRA	Integrated Resource Analyses
ITS	Intelligent Transportation System
LAN	Local Area Network
MANET	Mobile Ad-hoc Network
OBU	On Board Unit
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
RF-GPS	Referral node Global Positioning System
RSC	Road Side Controller
RSSI	Received Signal Strength Indicator
RSU	Road Side Unit
SOTIS	Self-Organizing Traffic Information System
TACNET	Tactical Network
TPM	Trusted Platform Module
VANET	Vehicular Ad-hoc Network
VIN	Vehicle Identification Number

VPKI	Vehicular Public Key Infrastructure
WANET	Wireless Ad-hoc Network