Indian Journal of Science and Technology, Vol 9(35), DOI: 10.17485/ijst/2016/v9i35/98094, September 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Defense against Prankster Attack in VANET Using Genetic Algorithm

Gaba Upma[1] and Saini Tanisha[2]

[1]CSE, Chandigarh Engineering College, Landran, Mohali - 140307, Punjab, India;
[2]CSE, Chandigarh University, National Highway 95, Chandigarh-Ludhiana Highway, Sahibzada Ajit Singh Nagar - 140413, Punjab, India; groverupma21@gmail.com, cecm.cse.tanisha@gmail.com

Abstract

Objectives: Detection and prevention of prankster attack in the network. One of the popular attacks in VANET is prankster attack that is affecting at high rate in the performance of the system. **Method**: In this paper, an algorithm based on genetic optimization has been presented for prevention as well detection of the attack. The genetic algorithm will work on the fitness function to prevent the prankster attack and the whole simulation will be done in MATLAB 2010 scenario. **Findings**: From the result evaluation it has been seen that proposed algorithm is better in terms of throughput, error rate, and delay and energy consumption. **Improvement**: Performance of the network get enhanced highly.

Keywords: Genetic Algorithm, Optimization, Prankster Attack, Security, VANET

1. Introduction

Security is very crucial topic these days in all networks to get high accuracy. So, in this section various sub topics will be considered like security in VANET, VANET Model, VANET settings etc.

A. Security in VANET

In recent years there has been growing interest in the field of VANET. There services basically fallen under security measures. Now a day's road traffic has become very crucial factor. Thus new developments for this is necessary for security purposes. Driving is one of the most important factor in which security is needed. Upcoming and accurate weather description is very important for drivers for safety precautions. VANETs are the subset of the MANET in which nodes are mainly vehicles. Data interchanged takes place in VANET in which security is very important. Data interchanging takes in terms of security. Such system must have high security. Figure 1 shows the VANET model. The crucial point of Vehicular Ad Hoc Network (VANET) deployment is to enhance the security in the network. Despite of high demand of security in network, there comes high security attacks called prankster attacks, which refers to the copy of the one physical identity namely Prankster nodes. In such circumstances, data received from malicious Prankster attacker may seem as if it was receive from many distinct physical nodes. Prankster nodes may deliberately mislead other neighbors, resulting in catastrophic situations like traffic jams or even deadly accidents. Preventing such attacks in a privacy-enabled environment is not a trivial task.

In this proposed, we aim to detect the Prankster attack in VANET. To cope with Prankster attack, we put forth a twofold strategy based Genetic Algorithm. The genetic algorithm will optimize the prankster nodes using fitness function. In the end proposed technique measurement will be done using basic matrices like throughput, Bit Error Rate, energy consumption and delay.

B. VANET Model Overview

Several various entities are assumed for the existence of VANET. Figure 1 shows the VANET Model. There are two types of environment of VANET:

*Author for correspondence

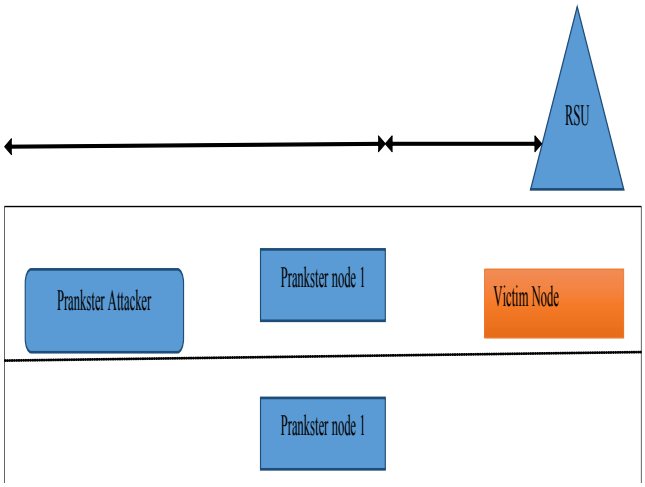

Figure 1. VANET Model.

- Infrastructure
- Ad hoc Network

C. VANET Setting

Following are the several application used in Vehicular Ad hoc network:

- V2V Warning Propagation:

Warning propagation of message to particular group.

- Group Communication of V2V.

Vehicles of same features participate in the group.

- V2V Warning

Messages are sent to know the danger in the area.

In the Figure 2(a), Figure 2(b) and Figure 2(c), orange circle denotes communicating nodes in the network ranging from n1 to nn. Blue colour circle represents the host. Similarly a black connected line is for communication interchanging between nodes.

D. Related Work

This section describes the work done by the number of authors in this field. Table 1 shows the comparison of the authors following their techniques and advantages.

In[1], introduced different contextual analyses for recognition of Sybil/prankster assault in VANET e.g. resource testing, position check and so forth. Vehicular specially appointed system may utilize settled cell doors and WLAN or WiMAX access for routing. In[2], exhibited the review of the effect of Sybil/prankster assault in VANET design.

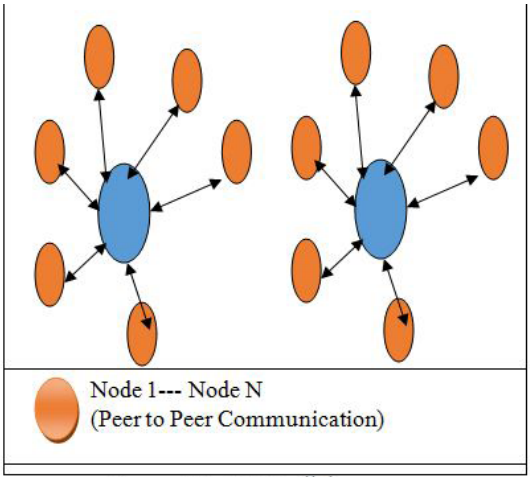

Figure 2(a). WAN cellular.

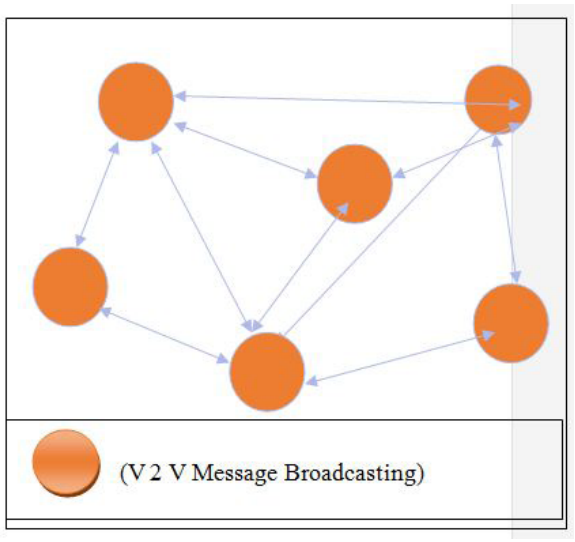

Figure 2(b). Pure ad hoc.

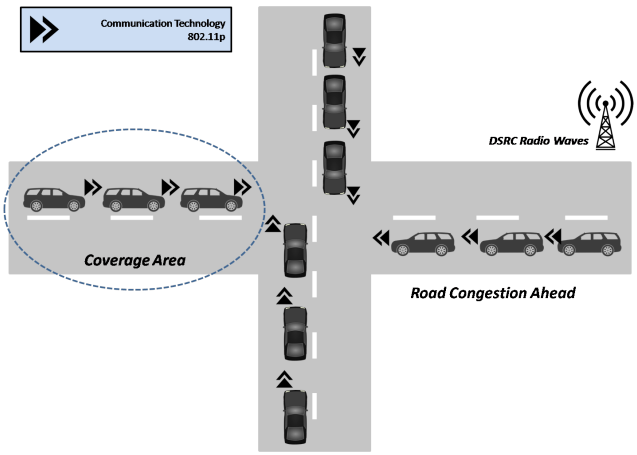

Figure 2(c). VANETs Mobility.

Table 1. Literature Comparison

Author	Year	Work Done	Conclusion
Ali Akbar et.al[11]	2014	Review of various selective techniques for Sybil attack detection.	Utilization of cell doors in VANET.
Priyanka Soni et.al[2]	2015	Review on Sybil attack.	Accuracy enhancement.
Rasheed et.al[3]	2012	Security review in VANET.	LMDS strategy provide high security.
Eman Farag Ahmed et.al[4]	2014	Routing protocols for attack prevention.	Black hole implementation is done in AODV, DSR and OLSR routing protocol.
Tyagi, P and Dembla[5]	2014	Investigation of security threat	VANET attacks their side effects
Reza et.al[6]	2014	ACO algorithm in VANET.	Avoid delay in the network.
Sumeet Sekhon et.al[7]	2014	Max-Min ant framework	Decrease in delay.
Ram shringar crude et.al[8]	2013	Security in VANET	Necessity of security in VANET described.
X.Sun et.al[9]	2007	Novel approach based on group signature and identify based signature.	Guarantees security and autonomy.
Raya et.al[10]	2007	Security architecture for detailed threat analysis	Privacy improved.
Ting Lu et.al[11]	2013	GA	Reduction in end delay.
K.S. Suresh[12]	2015	Free robot path planning (RPP) with GA.	RPP is effective and provide huge number of paths in environment.
Brindha et.al[13]	2015	Reformed Digital Micro Fluid Biochip	Minimize number of cells in array.
Jadhav Shital Suresh et.al[15]	2015	Security architecture around TPMs.	Hardware devices will improve the anonymity.
Arun Malik et.al[16]	2016	IAVIB-DP (Vehicle Initiated Broadcast-Dynamic Path)	More PI, High PDR, Low latency.

Sybil assault is a sort of security danger when a node in a framework ensures different characters. It is an assault wherein a malicious node gets inserted into other nodes. In[3], displayed the SADS system for avoidance of Sybil assault in VANET for dense traffic and LMDS strategy for less dense traffic. These plans gives cautioning signals at whatever point Sybil hub is found. Likewise they promise more security. In[4], proposed the VANET network in WSN system. Where hubs move freely in the network. In this paper the most common attack black hole in VANET has been demonstrated. The black hole implementation is done in AODV, DSR and OLSR routing protocol.

In[5], explored the security criteria in VANET. In this paper need of security in VANET has been presented. The basis VANET attacks has also been discussed here with their side effects. In[6], proposed ant colony optimization method for congestion in the VANET network to avoid delay in the network. In[7], introduced work based on swarm optimization algorithms utilizing Bio inspired calculations to recognize safe route over the entire system however notwithstanding this they have likewise utilized Max-Min ant framework (MMAS) to accomplish the objective of finding the ideal way for vehicles accordingly decreasing the delay. In[8], introduced the concept of security in the VANET. In this paper the need of security in VANET is demonstrated.

In[9], presented the method for the detection of black hole attack in the network. In proposed technique the main focus is to reduce the energy consumption in order to reduce the effect of black hole attack. In[10], present the concept of VANET. Various types of attacks has also been present in this article. In[11], introduced genetic algorithm to enhance the QOS services in the network. In proposed work GA enhancement is done to reduce the effect in parameters i.e. end to end delay etc.

II. Problem Analysis

In this section mathematical representation of prankster attack will be showed up;

```
xlocsy=[ ];
ylocsy=[];
for ti=1:myloopcount
dst=round(nodes*rand);
```

```
if dst==0
dst=10;
end
path_prankster(ti)=dst; %%%% clearing the prankster nodes each and every time
for g=1:dst
xlocsy(g)=1000*rand;
ylocsy(g)=1000*rand;
end
current_ratio_e(path_prankster(ti))=50*rand; %%%% energy of the current emtting node
end
hold on;
for ri=1:numel(path_prankster)
hold on;
try
plot(xlocsy(path_prankster(ri)),ylocsy(path_prankster(ri)),'ro','linewidth',3);
catch
end
```

III. Genetic Algorithm

The genetic algorithm is based on three factors and is invented by[11].

- Fitness function
- Selection function
- Crossover mutation

GA can be recognized in mathematical terms as below;

Let x(x1, x2…..xn) denote a binary vector. For notational

simplicity we restrict the discussion to binary variables xi= 0,1.

Let a function f: X→R >0 be given. We consider the optimization problem

Xopt= argmax f(x)

We will use f(x) as the fitness function. We will investigate two widely used recombination/crossover schemes. Using fitness function.

IV. Proposed Work

In this section, prankster attack prevention is taken place using genetic algorithm in VANET. Following algorithms will be adopted by us for solving the problem with the working flowchart that explains the whole working of the research. Figure 3 shows the working flowchart of the proposed work.

Algorithm1: Identification of Source & Destination

```
star=1;
message='Searching';
for i=1:10
path=[];
for k=1:star
message=strcat(message,' . ');
end
if star==4
star=1;
message='Searching';
end
star=star+1;
title(message);
pause(.0000003);
end
```

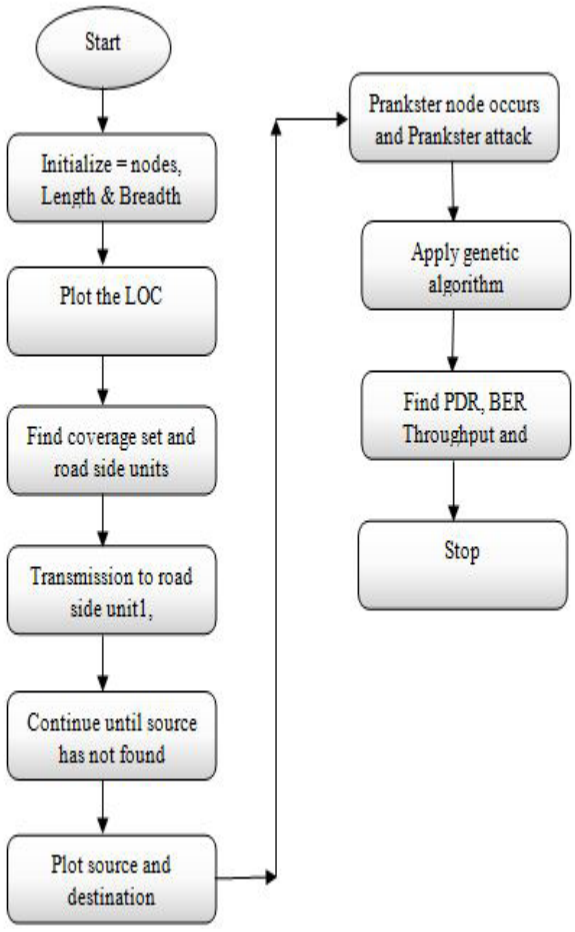

Figure 3. Work Flowchart.

Algorithm 2: Finding of Prankster Attack

```
xlocsy=[];
ylocsy=[];
for ti=1:myloopcount
dst=round(nodes*rand);
if dst==0
dst=10;
end
path_prankster(ti)=dst; %%%% clearing the prankster nodes each and every time
for g=1:dst
xlocsy(g)=1000*rand;
ylocsy(g)=1000*rand;
end
current_ratio_e(path_prankster(ti))=50*rand; %%%% energy of the current emtting node
end
hold on;
for ri=1:numel(path_prankster)
hold on;
try
plot(xlocsy(path_prankster(ri)),ylocsy(path_prankster(ri)),'ro','linewidth',3);
catch
end
title('prankster NODE Plotting');
pause(.0021);
title('');
end
title('prankster Node Plotted');
for i=1:20
pause(.55);
title('');
title('Searching in cache memory');
end
for fi=1:numel(path_prankster)
ds=find(pranksternodecache(:,:)==path_prankster(fi));
end
if ds>0
title('NODE FOUND IN THE CACHE MEMORY');
throughput(jst)=(packet_transferred(jst)-packet_loss_general(jst))/packet_transferred(jst);
myber(jst)=error_rate_general(jst);
 mydelay(jst)=delay_normal(jst);
 myenergy(jst)=energy_loss_general(jst);
else
throughput(jst)=(packet_transferred(jst)-((packet_loss_general(jst))+packet_loss_prankster(jst)))/packet_transferred(jst);
myber(jst)=error_rate_general(jst)+error_rate_prankster(jst);
mydelay(jst)=delay_normal(jst)+delay_prankster(jst);
myenergy(jst)=energy_loss_general(jst)+energy_loss_prankster(jst);
end
end
```

Algorithm 3: Fitness Function of Genetic Algorithm

```
function [ f] = fitness_fn( e,fs,ft )
FITNESS_FN Summary of this function goes here
Detailed explanation goes here
if fs<=ft
f=1;% if the current energy consumption is less than that of the overall energy consumption then 1 would be the output of this function else it would return 0
else
f=0;
end
end
```

V. Results and Discussions

A. Simulation Environment

This section deals with the network parameters used in the research work that is being shown in the Table 2.

B. Discussion

The graph shown in Figure 4 compares all values of throughput of different algorithms with respect to number of nodes. Throughput with GA shows the value from 25.1 to 26 and without optimization shows the value from -2 to 8. It shows that the result of GA algorithm is better than the comparison without GA.

As shown in Figure 5, all values of energy of different algorithms are compared with number of nodes. Energy with GA shows the value from 1.5 to 2.5 and without optimization shows the value from 7 to 22. It shows that

Table 2. Network Parameters

Environment	MATLAB 2010
Optimization algorithm	Genetic Algorithm
No. of nodes	20
Network size	1000* 1000
Parameters	Throughput, energy, delay and error rate.

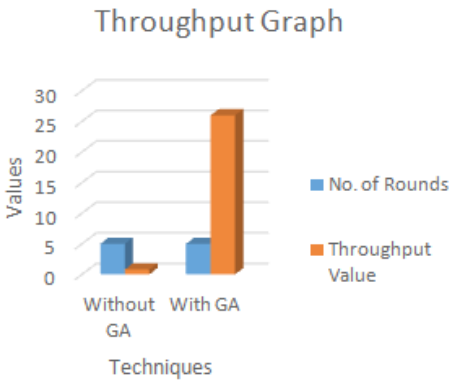

Figure 4. Comparison between throughput using GA and without GA.

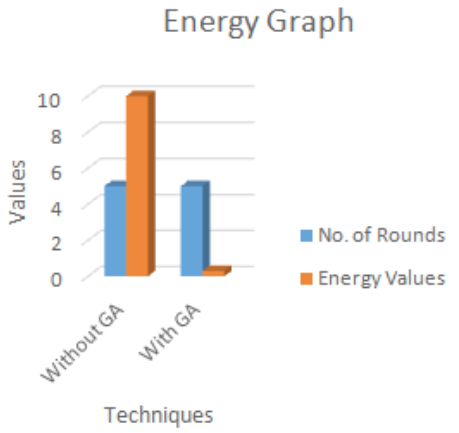

Figure 5. Comparison between energy using GA and without GA.

the result of GA algorithm is better than the comparison without GA.

The values of different algorithms have been compared in the Figure 6 taking number of nodes in bit error rate parameter. Error rate with GA shows the value from 2.7 to 6.3 and without optimization shows the value from 11 to 57. It shows that the result of GA algorithm is better than the comparison without GA.

Algorithms considered with GA and without GA have been compared with number of nodes in this work in Figure 7. Delay with GA shows the value from -3 to 1 and without optimization shows the value from 5 to 7. It shows that the result of GA algorithm is better than the comparison without BFO.

The comparison of proposed and the base algorithm[12] is shown in Table 3 that shows the comparison with respect to delay parameter. It shows that proposed work has delay of -0.3 and the base algorithm[t] has the delay of 0.036. It has been shown in Figure 8 graphically.

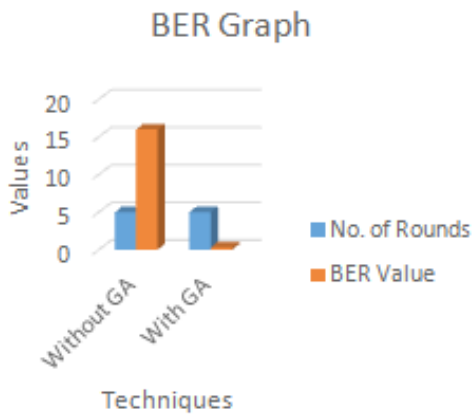

Figure 6. Comparison between error rate using GA and without GA.

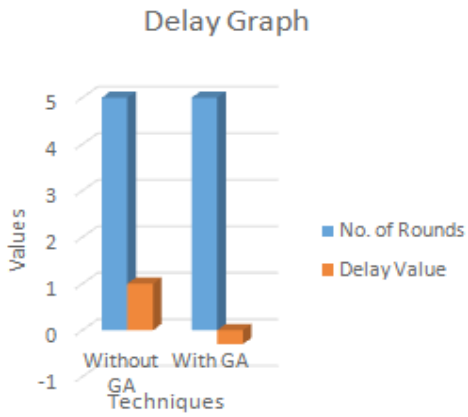

Figure 7. Comparison between delay using GA and without GA.

Table 3. Comparison of Graph Values

Technique	Delay
Proposed	-0.3
Mandeep Kaur [12]	0.036

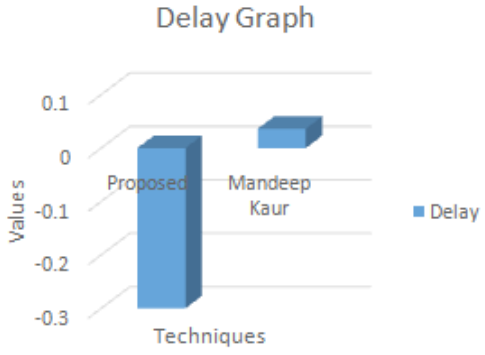

Figure 8. Comparison Graph.

VI. Conclusion and Future Scope

In this work, prankster attack detection using genetic algorithm (GA) has been shown using various metrics. So, an IDS system is built up in proposed work. The algorithm is tested for 20 nodes with 1000* 1000 network size. Genetic algorithm detected and prevented this attack using fitness function. In the end it has been concluded that GA based IDS system worked well.

Future scope lies in the usage of the other optimization method like PSO, BFO etc for other routing protocols too.

VII. Acknowledgement

Grateful acknowledgement is dedicated to Assistant Prof. Tanisha Saini and Dr. Vishal Sharma who contributed valuable comments in reviewing this paper.

VIII. References

1. Pouyan AA, Alimohammadi M. Sybil Attack Detection in Vehicular Networks. Computer Science and Information Technology. 2014; 2(4):197–202.
2. Soni P. A Review of Impact of Sybil Attack in VANET's. International Journal of Advanced Research in Computer Science and Software Engineering. 2015; 5(2):1–4.
3. Rasheed R. Springer: Privacy-Aware VANET Security: Putting Data-Centric Misbehaviour and Sybil Attack Detection Schemes into Practice. 2012; 7690:296–311.
4. Ahmed A, Farag E, Abouhogail RA, Yahya A. Performance Evaluation of Black hole Attack on VANET's Routing Protocols. International Journal of Software Engineering & Its Applications. 2014; 8(9):39–54.
5. Tyagi P, Dembla D. Investigating the security threat in vehicular ad-hoc Networks (VANETs): Towards security engineering for safer on road transportation. New Delhi: International Conference, Advances in computing, communication and Informatics (ICACCI). 2014; p. 2084–90.
6. Reza R. Ant-based Vehicle Congestion Avoidance System using Vehicular Networks. Engineering Applications of Artificial Intelligence. 2014; 36:303–19.
7. Sekhon S. Optimizing the Ad-hoc applications in Vehicular Network using Max-Min Ant system, International Journal of Engineering and Computer Science. 2014; 3(7):1–4.
8. Shringar R. Security Challenges, Issues and Their solutions for VANET. International Journal of Network Security & Its Applications (IJNSA). 2013; 5(5):95–105.
9. Sun X, Lin X, Ho PH. Secure vehicular communications based on group signature and ID-based signature scheme. Scotland, Glasgow: Proc. IEEE ICC. 2007; p. 37–41.
10. Raya M, Hubaux JP. Securing vehicular ad hoc networks. J. Comput. Security. 2007; 15(1):39–68.
11. Lu T, Zhu J. Genetic Algorithm for Energy-Efficient QoS Multicast Routing. IEEE Communications Letters. 2013; 17(1):31–35.
12. Kaue M. Movement Abnormality Evaluation Model in the Partially Centralized VANETs for Prevention Against Sybil Attack or prankster attack. I.J. Modern Education and Computer Science. 2015; 7(1):20–27.
13. Suresh KS, Vaithiyanathan V, Venugopal S. Layered Approach for Three Dimensional Collision Free Robot Path Planning using Genetic Algorithm. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–6.
14. Brindha G, Rohini G, Gnanakousalya C. Genetic Algorithm based Optimization of Single Node in Reformed-Digital Micro Fluidic Biochip. Indian Journal of Science and Technology. 2015 Nov; 8(29):1–8.
15. Suresh JS, Jongkun L. A TPM-based Architecture to Secure VANET. Indian Journal of Science and Technology. 2015 July; 8(15):1–6.
16. Malik A, Pandey B. An Intelligent Authentication Based Vehicle Initiated Broadcast-Dynamic Path Data Collection Scheme in VANET. Indian Journal of Science and Technology. 2016 Apr; 9(16):1–9.