A Review on Detection and Prevention of Prankster Attack using evolutionary Algorithm in VANET

Upma Gaba[1], Tanisha Saini[2]
[1]CSE, Chandigarh Engineering College, India
[2] CSE, Chandigarh University, India
groverupma21@gmail.com, cecm.cse.tanisha@gmail.com

Abstract — The most important fact in VANET (Vehicular Ad Hoc Network) is vehicle position. The original paths are changed by Prankster and Malicious attackers into fake packets and harm the VANET. It can be also termed as congestion in network. It has been seen very often that some malicious vehicles passes wrong information to the network through which the vehicles get distort from their original path. Previously various have been come out. But in this research , the advantage of genetic algorithm will be presented to detect the prankster attack.

Keywords—Prankster Attack, Genetic Algorithm(GA), Preventions, Security Concerns.

I. INTRODUCTION

As the wireless technologies are developing day by day, people are using the access of wireless anywhere. The car manufacturer and industries of telecommunication are using wireless technologies these days that are even helpful the road accidents and efficiency of traffic by bringing the IT services to the vehicles. VANET is the self organized network that gives the cars a wireless communication with the wireless communication strategies. It is a dynamic network that communicates with each other with networked vehicles [1]. They can even communicate by RSU's(Roadside Units) with the help of Short range communication method. They have OBU's (on board units) for performing the communication.

As per the best potential and the advantages of VANETs, gain has been taken place in academics and the industries and number of rules and regulations have been developed for the implementation of the approaches, their applications with the safety measures [1]. The fundamentally problem related to security is the Prankster Attack [4].

- **Present Scenario of security in VANET**

The node of VANET works as host and as router because of its decentralized nature. The topology of the network varies consequently as per the nature of the nodes. The traffic density also changes with the density of the network. By this, VANET become the challenging task to handle with. The main issue with respect to the security are: Data protection of sensors, safe communication, software and security alters the system. There can be number of attacks in VANET and it is mandatory that VANET can handle with every type of attack [9]. Because it's unique characteristics, framework of infrastructure ability and the less distance of the links in the nodes, VANET came out to be different from the other wired and wireless networks [11].

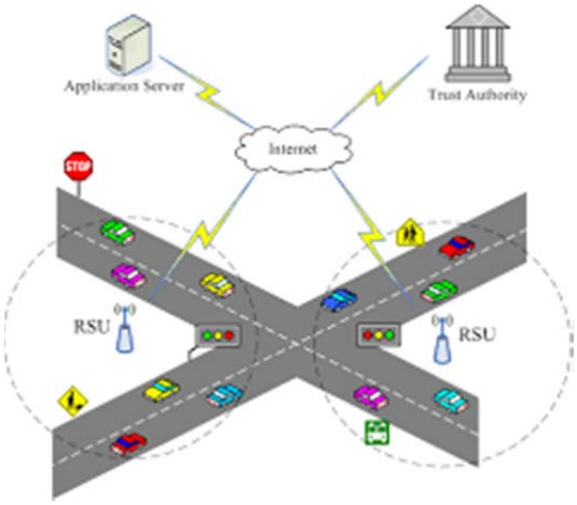


Figure. 1 Attack Scenario in VANET

- **Prankster Attack**

Prankster Attack is the one who wants to create negative impact on the network, and attacks in such a way that it plays with all the network users. All the users come under the wrong dilemma and are convinced to either increase or decrease their speeds [5]. False information is given to the nodes causing traffic congestion, not expected accident that could affect the rest of the local vehicles. The hallucination of the congestion of traffic before selecting the another destination for the advantage that might obtain by the attacker. MANET (Mobile adhoc network) obtain VANET that communication between the local nodes, among the nodes or local nodes that are side traffic management units RSU's. They has number of applications with MANETs like sudden variation in topology, more scaled, variable network density, no power constraint. The structure of VANET is obtained for V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) that areon RSU's and OBU's executed in vehicles. For collecting the data of the road, numbers of sensors are also used [6]

Security Concerns in VANET

For a safe and reliable VANET, variety of safety needs need to measure. A number of these security necessities are the similar for every network except a few of suitable and precise to VANE simply [7].

1. Authentication
2. Integrity
3. Non-Repudiation
4. Privacy
5. Availability

- **Advantages of VANET**

The usage of VANET is classified below:

1. Real-time group: The steady movement data could be used at RSU's and could be available to the vehicle at any point and any where required [8].
2. Co-agent Message delivery: Slow moving Vehicle would deal with the communication and co-work for helping number of vehicles. In spite of the truth that untiring value and dormancy will be of major concern, which might let things use similar to disaster brake to move possible mischance.
3. Post-Crash announcement: A vehicle built-in in an accident will broadcast cautionary communication concerning its place to irregular vehicles by the objective to have a choice by time with the power and in addition to thruway look for tow away support as displayed;
4. Road Hazard manage announcement: Cars advise dissimilar autos concerning road with flood or information concerning road highlight warning as of street bend, unexpected down and so onwards [9].
5. Cooperative crash caution: Alerts the drivers possibly be mishap way with the target that they could patch their behaviors.
6. Distant Vehicle Personalization/ Diagnostics: It is useful in downloading of modified vehicle setting or sending of vehicle diagnostics to bottom.
7. Internet contact: The Vehicles could have web during RSU's.
8. Digital direct downloading: Chart of locales could be downloaded by the drivers as per the requirement earlier than creating a journey to other area for journey way. Similarly, Content Map Database Download go on like an entrance intended for receiving gainful data starting flexible difficulty area.
9. Real Time Video communication: On-interest pictures knowledge will not be limited to the restrictions of the house and the driver is capable to demand constant characteristic move of the mainly appreciated movement movies.
10. Value-incorporated ad: This is mainly intended for the administration suppliers, who need to pull in clients to their stores. Declarations like petrol pumps, roadways eateries to declare their administrations to the drivers inside correspondence range. This application can be accessible even without the Internet.
11. Parking accessibility: Notifications for the accessibility of stopping in the metropolitan urban communities serves to discover the accessibility of openings in parking garages in a certain topographical territory [10].
12. Lively calculation: It expect the imminent geography of the street, which is required to improve fuel utilization by modifying the cruising speed before beginning a plunge or a climb. Besides, the driver is likewise helped

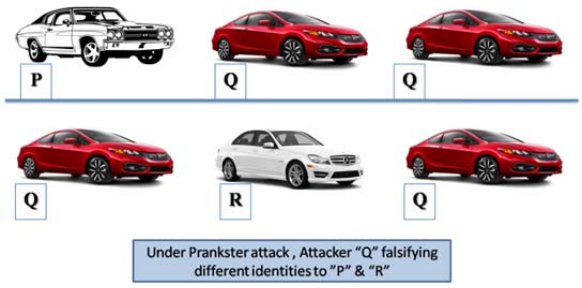
II. LITERATURE REVIEW

S.NO	Sybil Detection Method	Description	Merits	Demerits
1	Statistical Analysis [14] [18]	It is method in which data can explained, described & summarized and conclusions can be drawn	The main advantage is predictive analytics to anticipate future problems in network	It may have large sampling error, constructs of validity may not be good. Even if more association is establish in factor, several instance it doesn't show that it is grounds of attack occurrence.
2	Data Mining [23]	It is method to find out insight& knowledge for dataset which can help identify Sybil attack	Can work with variables which do not even have correlation	Large Data sets over head.
3	Data Stream Analysis [23]	It is the process of extracting knowledge structures from continuous, rapid data records in real time frame.	Get Response in Real time before Sybil attack might transport more difficult and could effort on Incremental heuristic investigation.	Large Data sets overhead, Limited offline analysis.
4	Machine Learning [17]	The difference in this case is NOT in the techniques of data mining or machine learning but in with the analysis, for machine learning, the structure of datasets to symbolize regular and irregular states to attain at a number of choices.	Works without explicit programming approach for detection of Sybil attack.	Not easy to work with unstructured large data in which unknown patterns are hidden.
5	Probability Based Method [21] [22]	It deals with problem that concerns both detecting whether or not a modification has taken place, or a number of changes that may occur, and finds the period of some changes that might helpful in finding the Sybil attack.	Used when there isn't an exhaustive population list available in real time for taking decision on Sybil attack.	More expensive and time-consuming over head
6	Sequence Mining [16]	Can discover the majority of common or uncommon patterns of activities	Can be used for Repeat-related problems	Over head of large dataset in terms of memory and retrieval /response time
7	Ranking {Trust, Reputation Voting } [15] [19]	In this method Trust points are given based on some algorithm, which helps to detection malicious nodes	Machine to machine voting system and man to machine voting systems of trust can be build	A Compromised network will lead to failure of the trust system.
8	Thresholding [20]	In this dynamic Thresholding algorithm with heuristics evaluation can be used for detection of Sybil attack	Simple to implement	Wrong calculation of thresholds due to large variability may lead to numerical stability problem of algorithm.

III. PROBLEM FORMULATION

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 accuracy, throughput, Bit Error Rate, Packet Delivery Ratio.



IV. UTILIZATION OF GENETIC ALGORITHM (GA)

In above literature survey various methods has been presented with their advantages as well as disadvantages, but it has been seen that evolutionary algorithms worked well so they are presented here.

The Genetic algorithm is an optimization process based on law of evolution and it has three operations basically i.e. *Selection, Genetic Operation,* and *Replacement* [24].A typical GA cycle is shown in Fig.2

The population consists of chromosomes. Each chromosome is selected from a population using fitness function.

Following algorithm has been adapted by GA:

```
Generate initial population X= x1, x2…..xn.
Compute fitness function fx.
Create new chromosomes
Delete old chromosomes from population to make new chromosomes.
Compute fitness function fx.
Go to compute fitness function step otherwise stop.
```

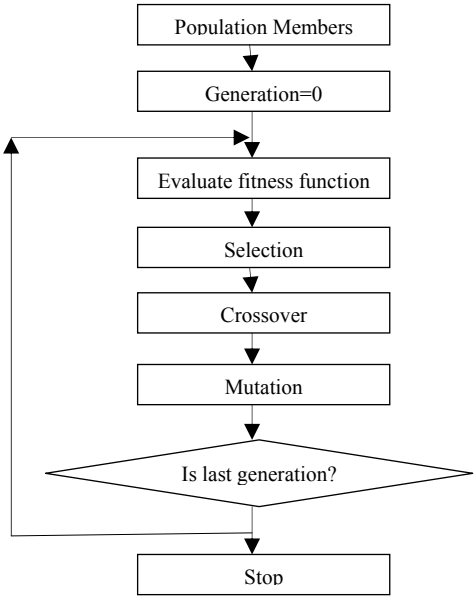


Figure. 2 Genetic Algorithm Flowchart

When the reduced feature set according to the fitness function is achieved, optimized results of QOS parameters are achieved. More throughput percentage, more battery life, more network life, minimum delay and minimum error rate are produced by using Genetic Algorithm. GA uses the simulated binary crossover operator and polynomial mutation. Simulated binary crossover operator can be represented below:

$$v1, l = \frac{1}{2}[(1 - N_l)a_{1,l} + (1 - N_l)a_{1,l}]$$

v2, l = $\frac{1}{2}[(1 + N_l)a_{1,l} + (1 - N_l)a_{2,l}]$,

Where v_1, l is the child of l component $a_{1,l}$ is the selected parent and N_l can be represented as below in terms of density;

A (B) = $\frac{1}{2}[(M_v + 1)B^{mv}$ if 0 <B <1

A (B) = $\frac{1}{2}[(M_v + 1)\frac{1}{B^{mv+2}}$ if B > 1

This uniformity can be described as:

B (i) = $(2i)^{\frac{1}{m+1}}$

V. METRICS

- **Throughput**

Throughput is the rate of invention or the rate on which a bit can be processed. When used in the framework of communication networks.

- **Packet Delivery ratio**

Packet delivery ratio is defined as the ratio of data packets expected by destinations to those generated through sources. It can be taken as :

PDR= S1÷ S2

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source

- **End to end delay**

The average time taken by data packet to reach the destination and includes all delays caused by buffering during route discovery latency, queuing at the interface queue. Mathematically, it can be defined as:

Avg. EED=S/N

S is the amount of the time spends to bring packet for each destination, and N is the number of packets received by the all destination nodes.

- **Routing overhead**

It is the ratio between the numbers of sent routing packets over the number of received data packets.

- **Bit Error rate**

The bit error rate (BER) is the numeral of bit errors per unit time. BER is a unit less calculation, frequently taken as percentage.

- **Congestion**

It occurs when a link or node having much data that its quality of service suffers. Typical effects include loss of packet, new connection blocking etc.

VI. CONCLUSION AND FUTURE SCOPE

These days various VANETs technologies are coming up due to the increasing demand of road safety. VANETs can be used in various fields because of its robustness feature like traffic signaling, road emergency warning etc. As if we do not consider the security factor then it will become very difficult to deploy such networks. So this paper has presented the utilization of genetic algorithm to solve the problem of prankster attack in VANET.

Abbreviations and Acronyms

RSU- Road Side Unit

QOS- Quality of Service

PDR-Packet Delivery Ratio

EED-End to End Delay

BER-Bit Error Rate

ACKNOWLEDGMENT

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

REFERENCES

[1] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures"Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" (IEEE,2010).
[2] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".
[3] Muhammad A. Javedand Jamil Y. Khan "A GeocastingTechnique in an IEEE802.11p based Vehicular Ad hoc Network for Road Traffic Management". (2010).
[4] Chia-Chen Hung, Hope Chan, and Eric Hsiao-KuangWu "Mobility Pattern Aware Routing for
[5] Heterogeneous Vehicular Networks"(IEEE WCNC 2008).
[6] João A. Dias, João N.Isento, Vasco N. G. J. Soares, FaridFarahmand, and Joel J. P. C. Rodrigues "TestbedbasedPerformance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks" (2011 IEEE).
[7] Steffen Moser, Simon Eckert and Frank Slomka "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks" 2012 IEEE.
[8] Irshad Ahmed Sumra, HalabiHasbullah, J.AbMananMohsanIftikhar, Iftikhar Ahmad, Mohammed Y Aalsalem "Trust Levels in Peer-to-Peer (P2P) Vehicular Network"2011 IEEE.
[9] Irshad Ahmed Sumra, HalabiHasbullah, JamalullailAbManan, "VANET Security Research and Development Ecosystem", 2011 IEEE.
[10] Lu Chen, Hongbo Tang, Junfei Wang, "Analysis ofVANET Security Based on Routing Protocol Information", 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)June 9 – 11, 2013, Beijing, China pp.134-138.
[11] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.
[12] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE ICC, Beijing, China, May 2008, pp. 1451–1457.
[13] X. Lin, "Secure and privacy-preserving vehicular communications," Ph.D. dissertation, Univ. Waterloo, Department of Electrical and Computer Engineering, Waterloo, ON, Canada, 2008.
[14] Dotzer F, Fischer L, Magiera P (2005) Vars: a vehicle ad-hoc network reputation system. In: IEEE international symposium on a world of wireless mobile and multimedia networks,pp 454–456
[15] .Feiri, M.; Petit, J.; Schmidt, R.K.; Kargl, F., "The impact of security on cooperative awareness in VANET," in Vehicular Networking Conference (VNC), 2013 IEEE, vol., no., pp.127-134, 16-18 Dec. 2013
[16] Sayegh, N.; Elhajj, I.H.; Kayssi, A.; Chehab, A., "SCADA Intrusion Detection System based on temporal behavior of frequent patterns," in Mediterranean Electro technical Conference (MELECON), 2014 17th IEEE, vol., no., pp.432438, 13-16 April 2014.
[17] AlMheiri, S.M.; AlQamzi, H.S., "MANETs and VANETs clustering algorithms: A survey," in GCC Conference and Exhibition (GCCCE), 2015 IEEE 8th, vol., no., pp.1-6, 1-4 Feb. 2015.
[18] Mukherjee, B.; Heberlein, L.T.; Levitt, K.N., "Network intrusion detection," in Network, IEEE, vol.8, no.3, pp.26-41, May-June 1994.
[19] Krishna, T.R.V.; Barnwal, R.P.; Ghosh, S.K., "MDS-Based Trust Estimation of Event Reporting Node in VANET," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, vol., no., pp.315-320, 16-18 July 2013.
[20] Tong Zhou, Romit Roy Choudhury, Peng Ning, and KrishnenduChakrabarty., P2DAP – "Sybil Attacks Detection in Vehicular Ad Hoc Networks", IEEE journal on selected areas in communications, vol. 29, no. 3, march 2011.
[21] Erritali, M.; El Ouahidi, B., "A review and classification of various VANET Intrusion Detection Systems," in Security Days (JNS3), 2013 National, vol., no., pp.1-6, 26-27 April 2013.
[22] Raut, S.B.; Malik, L.G., "Survey on vehicle collision prediction in VANET," in Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on, vol., no., pp.1-5, 18-20 Dec. 2014.
[23] Jeong, H.J.; WooSeok Hyun; Jiyoung Lim; Ilsun You, "Anomaly Teletraffic Intrusion Detection Systems on Hadoop-Based Platforms: A Survey of Some Problems and Solutions," in NetworkBased Information Systems (NBiS), 2012 15th International Conference on, vol., no., pp.766770, 26-28 Sept. 2012.
[24] Ajay Rawat, Santosh Sharma, Rama Sushil, "Vanet: Security Attacks and its Possible Solutions," Journal of Information and Operations Management, Volume 3, Issue 1, pp301-304, 2012.
[25] Ting Lu and Jie Zhu, "Genetic Algorithm for Energy-Efficient QoS Multicast Routing", IEEE Communications Letters, Vol.17, pp. 31-35, 2013.

AUTHORS PROFILE

Upma Gaba is currently a student at Computer Science Department in Chandigarh Engineering College, Chandigarh, India. She received an engineering degree in year June 2013 in C.S.E. Her research interests include networking and communications in ADHOC networks with specialisation in VANETS. The implementation part is done with MATLAB tool.

Tanisha Saini, an Assistant Professor at Computer Science Department in Chandigarh Engineering College, Chandigarh, India. She received an engineering degree in year June 2012 in C.S.E. Her research interests include networking and communications in WSNs with specialisation in VANETS. The implementation part is done with NS2 tool.