Optimizing the Potential Attacks through Safety and Secrecy in Vehicular Ad Hoc Networks

M. Anbukkarasi[1] M. Selvalakshmi[2]
[1]Assistant Professor [2]Research Scholar
[1,2]Department of Computer Science & Information Technology
[1,2]S.S. Duraisamy Nadar Mariammal College, Kovilpatti, Tamil Nadu, India

Abstract— Now-a-days Ad Hoc network is the greatest prominent research area for the researchers. VANET act as a major role to communicate the vehicles through Road Side Unit (RSU) which is interrelated about the traffic jam, collision between the vehicles and safety. It faces many real time problems during the communication such as bogus information, Imposture, DoS, Surveillance etc., This paper resolves the problem which is related to safety and secrecy. Major safety concerns include privacy, integrity and availability. It faces the concerns such as high agility, position detection and trust group formation. Confidentiality in VANET focuses on sensitive information, illegal tracing and user outlining for commercials. In this paper we focus to optimize the security and privacy challenges to achieve protection of life.

Key words: DoS, Optimization, Privacy, Road Side Unit, Safety, Security, VANET

I. INTRODUCTION

The rapid advancement in wireless communication networks has made it possible for Inter-Vehicular Communications (IVC) and Road-Vehicle Communication (RVC) in Mobile Ad Hoc Networks (MANET). This led to the innovation of new type of MANET known as Vehicular Ad Hoc Network (VANET) to improve road safety, better traffic, proficient driving and infotainment. Every node can move easily within the available network and be in connection. A node can communicate with other nodes and it could be a vehicle or a Road Side Unit (RSU) is gateways that allow vehicles to establish connection with internet. This is the stationary part of the network. The RSU is equipped with one network device for a dedicated short range communication based on IEEE 802.11.

The main tasks of RSU are as follows:

1) Extending the network coverage and enabling exchange of information between communicating OBUs and RSUs.
2) RSU acts as a source of information.
3) RSU helps the OBUs to get connected to internet.

Now that the number of vehicles increased exponentially and millions of people get injured, moreover traffic congestion makes a huge wastage of time and fuel.

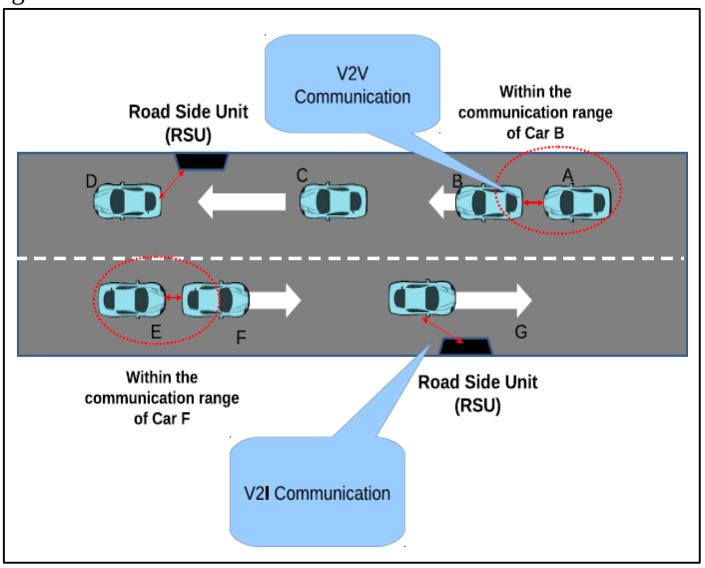

Fig. 1: VANET Structure

VANET safety should satisfy four goals, it should ensure that the information received is correct, the source is who he claims to be, the node sending the message cannot be identified and traced (secrecy) and the system is robust.

II. SURVEY ON SAFETY AND SECRECY PROPOSALS

Lot of efforts has been made by investigators in the security and privacy concerns of VANET worldwide. Some of them are:

According to Bharathi Mishra [1] the concept of vehicular network was first proposed by a team of engineers from Delphi Delco Electronics Systems.

Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux and Antonio Lioy [3] in 2007 proposed solutions to concerns as effect of the security and the pseudonym-based mechanisms on safety solicitations to meet the security and privacy requirements.

Tony K. Mak, Kenneth P. Laber teaux, Raja Sengupta [4] in 2005 formulated a protocol design for Multichannel VANET Providing Concurrent Safety and Commercial Services They proposed safety requirements while supporting non-safety communications.

Yi Yang, Rajive Bagrodia, [5] Mobile Systems Lab, Computer Science Department, University of California, Los Angeles proposed Evaluation of VANET-based Advanced Intelligent Transportation Systems that integrate wireless network with transportation providing a user level recreation environment to evaluate the probability and performance limitations of VANETs.

Nattiya Khaitiyakunand Teerapat Sanguan kotchakorn [6] of Asian Institute of Technology Pathumthani, Thailand in the year 2014 proposed an analysis of data diffusion on VANET by using Content Delivery Network (CDN) technique. They proposed a method to apply the CDN technique for data dissemination from a single source node to multiple destinations in VANET environment. Tracy Ann Kosa, Stephen Marsh and Khalil El-Khatib [7] published a paper on privacy representation in VANET. They proposed a framework for secrecy representation.

III. WHY WE NEED SAFETY AND SECRECY?

Safety and confidentiality are essential challenges in today's life. Any unauthorized user can detect the data and corrupt it and change the actual data, so that receiver will get wrong data. Through neighbour identity authentication, user can validate their identity whether it is authorized or not.

A. Safety Concerns in VANET

VANET suffer from various attacks, the following are certain potential attacks [2] of vehicular networks they are:

1) *Bogus information* – attackers send inaccurate information into the network to affect the behavior of other drivers.
2) *Imposture*- attackers pretend to be other vehicles by using incorrect identities.
3) *Denial of Service*-attackers may want to bring down the vehicular network [14] or even cause an accident. DoS attacks can be carried out in many ways [8].

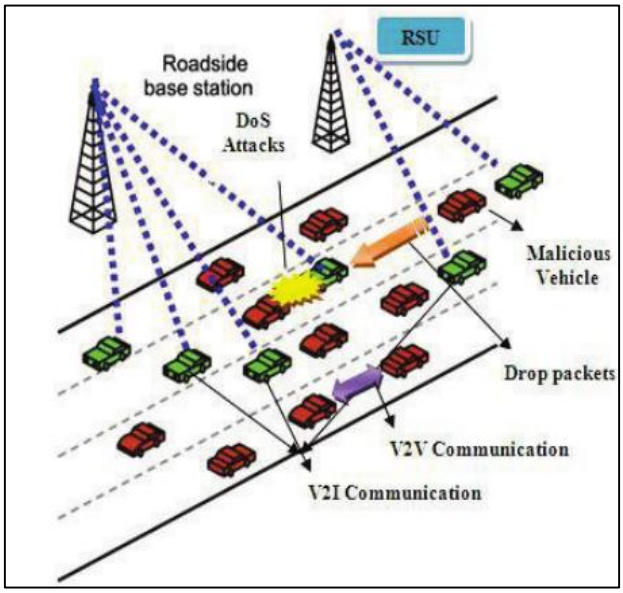

Fig. 2: DoS attack in VANET

4) *Surveillance*- Vehicle Shelter communication technology leads to increased scrutiny of drivers appealing in everyday activities on the public roads.
5) *Reply legitimate messages*- It may be intercepted and replayed at a dissimilar time and/or at different locations.

IV. SECRECY CONCERNS

A very dangerous and often ignored fact about privacy is that innocent looking data from various sources can be accumulated over a long period and evaluated automatically. Even small correlations of the records may expose useful information. For instance, the data about specific sensor characteristics may give some suggestions about the make and the model of car. This in turn may be related to other information to identify a specific car. And once privacy is lost, it is very hard to re-establish that state of personal rights.

The profile or a driver's personal information must be maintained against unauthorized access. We consider the following two cases:

- Communications between vehicles and RSUs.
- Communications between vehicles.

V. INTRUDERS ON NETWORK

To secure the VANET, first we have to find who are the attacker, their nature, and capability to damage the system. Basically these attackers may be three types [9].

•Insider and Outsider: Insiders are the authenticated members of network whereas Outsiders are the intruders and has limited capacity to attack.
•Wicked and Rational: Wicked invaders harm the functionality of the network. Rational aggressors have the personal profit hence they are predictable.
•Active and Passive: Active attackers generate indicators or packets whereas passive attackers only sense the network.

SAFETY APPLICATION

It compacts with all safety related concerns like road conditions, monitor other vehicles in the network etc. This informs other vehicles in the network about these situations and broadcasting feature is used. Some of the protection applications are discussed below:

Vehicle Consultant – It can send warning signals/messages to the surrounding vehicles in the network [1].

Post-Crash Notifications- Vehicles met with accidents can broadcast messages about its position to neighboring vehicles and also seeking help to highway guard.

Collision Avoidance-Improving collision avoidance application reduces road accidents. By rising sensors at the RSU information can be collected, processed and warning messages can be forwarded to the vehicles to avoid crash.

SAFETY REQUIREMENTS

In this section, we present the main security requirements for VANETs [10], [11], [12], [13]. Three properties regarding security that cannot be ignored are privacy, integrity, and availability.

Privacy

In VANETs, privacy refers to "confidential communication" [10]. In a group, none except group members are able to decrypt the messages that are broadcasted to every member of group and none (even other members) except a dedicated receiver member is capable to decrypt the message devoted to it.

Integrity

It ensures that data or messages delivered among nodes are not altered by attackers. This concept in VANETs often combines with the concept "authentication". Once the sender vehicle is authenticated, the receiving vehicle performs data verifications to check whether the message contains the correct or corrupted data.

Availability

The network should be available even if it is under an attack without affecting its performance.

VANET CHALLENGES

A VANET environment has to overcome assured concerns of drawback and inadequacy. It includes [15]:
Limited Range of Wireless Transmission.
There are transmission disorders like path harm, dying, obstacle and intervention that introduce susceptible nature of wireless medium.
Packet Losses Due to Errors in Transmission.
Path Changes Due to Mobility.
Frequently used network Partitions affects the intermediary devices.
Energy Efficiency is operated by batteries. So it is a major concern to save power or energy for frequent data packet forwarding from source to destination.

IV. PROPOSED IMPROVED PARTICLE SWARM OPTIMIZATION (IPSO) ALGORITHM

To overcome the problem in VANETs, the potential attacks through safety and secrecy are needed to be optimized by using proposed improved particle swarm optimization algorithm.

Starting with a random set and moving in arbitrarily chosen directions, each particle are carried out through the searching space while remembering the best positions it has seen. Members of particles of swarm communicate their positions to each other as well as dynamically adjust their own position and velocity derived from the best position of all particles. As

soon as a particle finds the best solution, it starts influencing its neighbors. Finally, all particles incline to fly towards better positions over the searching process until the swarm move to close to an optimum of the fitness.

In IPSO, each particle flies through the multidimensional space and adjusts its position in every step that toward an optimal solution by the entire swarm. Therefore, the IPSO algorithm is a member of Swarm Intelligence [16]. IPSO bonds many resemblances with Genetic Algorithms, which is one of the evolutionary computation techniques, except that IPSO has no development operators such as crossover and transformation.

Improved Particle Swarm Optimization algorithm transitions particles in a realistic and probabilistic space using the velocity of the particle. The swarm tries to maximize the probability of a certain binary variable such that its probability is exploited. The algorithm uses the velocity update equation as in [1] but the values of 'X' are now randomly discrete and binary. For position update, first the velocity is transformed into an [0, 1] interval using the sigmoid function given by

$$S_{id} = sig\,(V_{id}) = 1/1+e^{-Vid} \quad (1)$$

where, V_{id} is the velocity of the i^{th} particle's d^{th} dimension. A number is produced using an even distribution which is compared to the value generated from the sigmoid function and the X_{id} is calculated as:

$$X_{id} = u\,(S_{id} - U\,[0, 1]) \quad (2)$$

u is a unit step function. The decision regarding X_{id} is probabilistic, implying that larger the value of the V_{id}, greater the value of the S_{id}, making probability of deciding '1' for X_{id} higher. It should be noted that as $V_{id} \to \infty$, $S_{id} \to 1$, making it impossible X_{id} to return to zero after that point. Until that point there is some probability of X_{id} returning to zero. Figure 3 shows this property of the improved particle swarm optimization. The probability of X_{id} =1 increases as V_{id} increases. However, P (X_{id}=1) is almost equal to 1 for V_{id}>10, but is not exactly equal to 1. This is the key to the design of the discrete improved particle swarm optimization, since particles do not get trapped once they find optima.

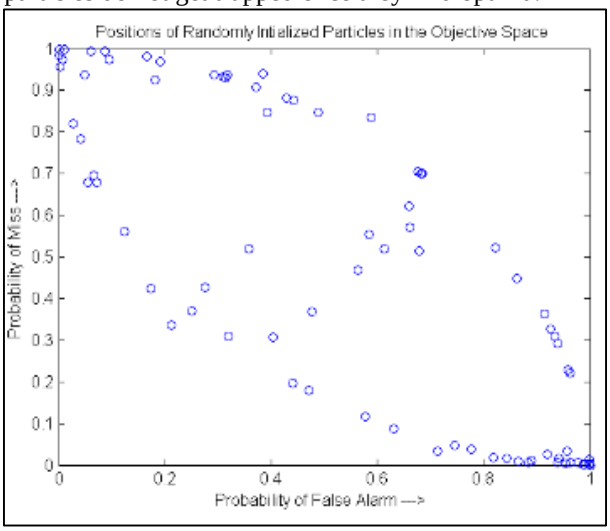

Fig. 3: Randomly set particles

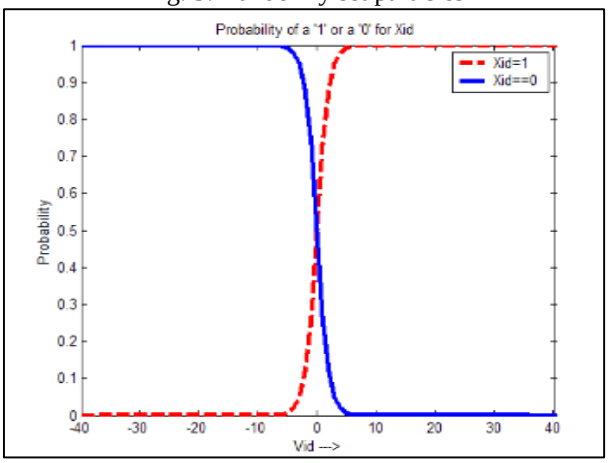

Fig. 4: Transformation of the Particle Velocity to a Binary Variable

	K		T_1		T_2		T_d		No. of Gen.	CPU Time (sec)
	Value	% diff.	value	% diff.	value	% diff.	value	% diff.		
Genetic Algorithm										
No noise	7.600	0.0%	10.006	0.07%	*n/a*	*n/a*	24.992	-0.03%	47	306.4
With noise	7.602	0.03%	10.330	3.3%	*n/a*	*n/a*	25.372	1.5%	46	308.7
No noise	5.700	0.0%	43.380	7.9%	4.379	4.2%	41.072	-2.2%	100	306.0
With noise	5.706	0.1%	41.218	2.5%	4.313	2.7%	41.856	-0.3%	40	314.9
Particle Swarm Optimisation										
No noise	7.945	4.5%	10.972	9.7%	*n/a*	*n/a*	25.109	0.4%	54	365.3
With noise	7.808	2.7%	10.831	8.3%	*n/a*	*n/a*	24.948	-0.2%	56	365.7
No noise	5.668	-0.6%	44.102	9.7%	3.840	-8.6%	42.860	2.1%	89	353.5
With noise	5.575	-2.2%	25.536	-36.5%	3.158	-24.8%	43.389	3.3%	100	356.5

Table 1: Effects of applying the genetic algorithm and improved particle swarm optimization algorithm

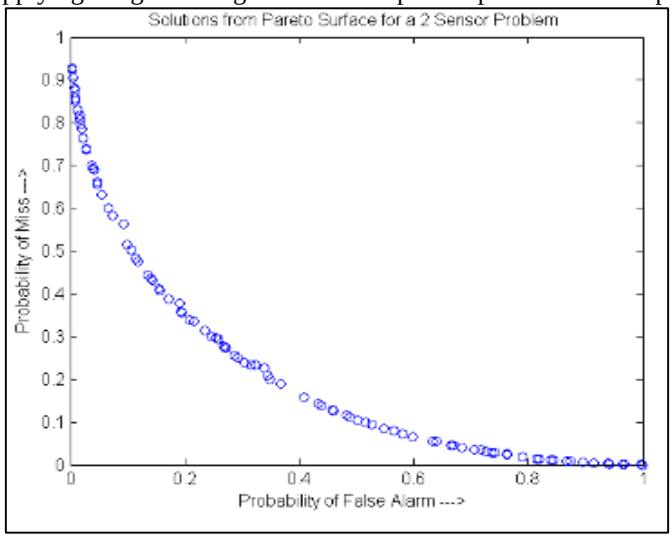

Fig. 5: Solutions from Pareto Surface for a two Sensor Problem

VI. CONCLUSIONS & FUTURE WORK

The simulation results show that the proposed algorithm is better in convergence speed and local minimum value, which shows that the improved particle swarm optimization algorithm has a good reference value. Thus Vehicular Ad Hoc Network gives plentiful chances for invaders, who will try to challenge the network with their malicious attacks.

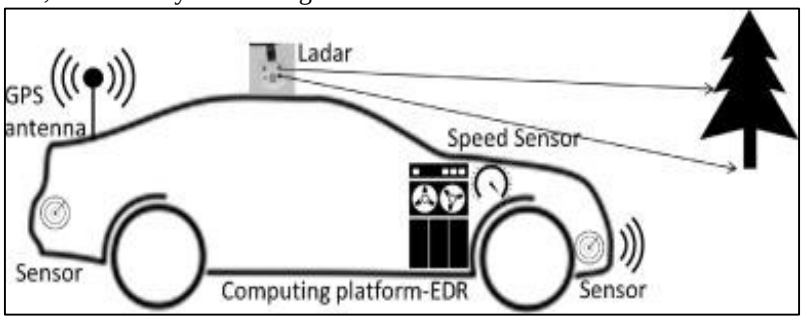

Fig. 6: Upcoming Design of VANET

In the upcoming years, vehicles in VANET will be equipped Global Positioning System, Event Data Recorder and sensors such as radar and ladar as shown in Fig.6. These are used to sense traffic blockings and status. Then repeatedly take proper actions in vehicle.

REFERENCES

[1] "Security in Vehicular AdHoc Networks: A Survey", Bharathi Mishra et al.
[2] S. Singh and U. Parmar, "Overview of various attacks in VANETs". *International Journal of Engineering Research and General Science*, 2015, pp. 3(3), 120-125.
[3] "Efficient and Robust Pseudonymous Authentication in VANET", Giorgio Calandriello et.al, Laboratory for Computer Communications and Applications, EPFL, Switzerland.

[4] "A MultiChannel VANET Providing Concurrent Safety and Commercial Services", K. Tony Mak, Kenneth, et al. University of California.
[5] "Evaluation of VANET-based Advanced Intelligent Transportation Systems", Yi Yang, Rajive Bagrodia
[6] "An Analysis of Data Dissemination on VANET by using Content Delivery Network (CDN) technique". Nattiya Khaitiyakun and Teerapat Sanguankotchakorn of Asian Institute of Technology Pathumthani, Thailand.
[7] "Privacy Representation in VANET", Tracy Ann Kosa, Stephen Marsh and Khalil El-Khatib, 2013.
[8] C. S. R. Murthy, B. S. Manoj : "Ad Hoc Wireless Networks: Architectures and Protocols". PEARSON, ISBN 81-317-0688-5, (2011).
[9] Maxim Raya e al., "The Security of Vehicular AdHoc Networks", SASN'05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21.
[10] Tat Wing Chim, S.M. Yiu, L.C.K. Hui and V.O.K Li, "Security and Privacy Issues for Inter-vehicle Communications in VANETs", in Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009, pp. 1-3.
[11] Lei Zhang, "Research on Security and Privacy in Vehicular Ad Hoc Networks", in PhD thesis at Universitat Rovira i Virgili, June 2010.
[12] Privacy International, [Online] Available: http://www.privacyinternational.org/indexs.html, Clerkenwell, London, (1990).
[13] "Vehicular Ad Hoc and Sensor Networks—Principles and Challenges". International Journal of Ad Hoc, Sensor & Ubiquitous Computing (IJASUC), 2,2011.
[14] H. Hasbullah, I. A. Soomro, J. A. Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", 2010, vol 4, pp 350-354.
[15] Sabih Ur Rehman et al., (2013). Vehicular Ad Hoc Networks (VANETS): An overview and challenges, journal of wireless networking and communications, 3(3), 29-38.
[16] Moayed D, Gary G Y. Cultural-Based Multi-objective Particle Swarm Optimization [J]. IEEE Transactions on Systems, Man and Cybernetics-Part B: Cybernetics, 2011, 41(2):553–567.