Using Particle Swarm Optimization (PSO) Algorithm to Protect Vehicular Ad Hoc Networks (VANETS) From Denial of Service (DOS) Attack

Silas Momanyi Nyabuga, Dr. Wilson Cheruiyot, Dr. Michael Kimwele

***Abstract*—** Vehicular ad hoc technology is a subset of mobile networks (MANETS) where vehicles are considered to be nodes communicating. A network of moving vehicles is established for a specific need or situation. Security has become an indispensable matter of attention in the Vehicular Ad-Hoc Network (VANETS), which is vulnerable to many security threats. One of the security threats is the Denial of Service (DoS) attacks, where a malicious node forges a large number of fake identities .To guarantee this security, network availability is inevitable. The network availability enhances node to node communication. The network is prone to many security challenges. The Denial of Service attack (DOS) on the VANETS is among the most venomous attacks on the network. DOS attacks aims at degrading the availability and quality of the network, in this case the attackers can potentially flood entire network so that no one will be able to use the applications/services and prevent the legitimate nodes from accessing services or resources such situations can create catastrophic situations if triggered. This paper aims at providing a review and discussions of the DOS detection and prevention mechanisms, moreover it intended to propose the PSO algorithm used to detect and prevent DOS in VANETS. Despite the many efforts towards prevention of the DOS attacks, it still remains a major concern. In this paper various methods of prevention and detection are discussed and a more reliable method has been presented.

***Index Terms*—** Particle Swarm Optimization (PSO), Vehicular ad hoc networks (VANETS), Denial of Service (DOS), Mobile networks (MANETS)

I. INTRODUCTION

Vehicular ad hoc networks (VANETS) is a mobile network technology where two or more vehicles communicate with each other or with an infrastructure i.e. a vehicle can communicate with another vehicle directly which is called vehicle to vehicle (V2V) communication or a vehicle can communicate to an infrastructure such as a road side unit (RSU) known as vehicle to infrastructure (V2I) [1]. Figure 1 shows a typical VANET scenario. VANET technology is emerging technologies to achieve inter-Vehicle communication that results in improved road safety and essential alerts. VANET serves the user with safety and non safety applications but needs security to implement the wireless environment. In VANET vehicles does not have fixed infrastructure because of the reasons that vehicles are mobile nodes [2].

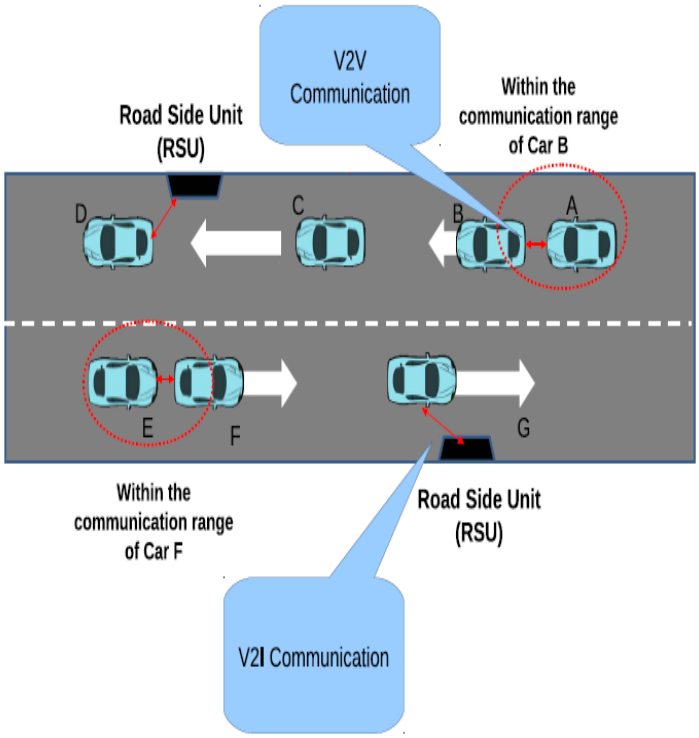

Figure 1: Creating an Adhoc network using vehicles [1].

II. DENIAL OF SERVICE ATTACK IN VANETS

A denial of service attack is the deliberate attempt by an attacker to prevent a legitimate user of a service from using the intended service [3]. Such an attack occurs when a targeted node (a vehicle in this case) is flooded with packets thus overwhelming the bandwidth of the victim node and preventing it from using its resources. Typically VANETS operate in wireless environment. In this environment the attacker attacks the communication medium to cause the channel jam or to create some problems for the nodes from accessing the network. The aim is to prevent the legitimate nodes from accessing the network services and from using the network resources; ultimately the networks are no longer

Manuscript received March, 2016.
Silas Momanyi Nyabuga, *Department of Computer Studies, The Kisii National Polytechnic, P.O. Box 222-40200, Kisii, Kenya.*

Dr. Wilson Cheruiyot, *School of Computing and information Technology (SCIT), Jomo Kenyatta University of Agriculture and Technology (JKUAT), P.O. Box 62000, Nairobi , Kenya .*

Dr. Michael Kimwele, *School of Computing and information Technology (SCIT), Jomo Kenyatta University of Agriculture and Technology (JKUAT), P.O. Box 62000, Nairobi , Kenya .*

ISSN: 2278 – 1323

available to legitimate nodes. The DOS attacks can be achieved through communication channel jamming, network overloading and packets dropping [4]. The DOS attack is the most serious level attack in vehicular networks as it jams the communication medium and consequently denies the legitimate users from accessing the network and other network resources [2]. Figure 2 below depicts the whole scenario when the attacker A launches a DOS attack.

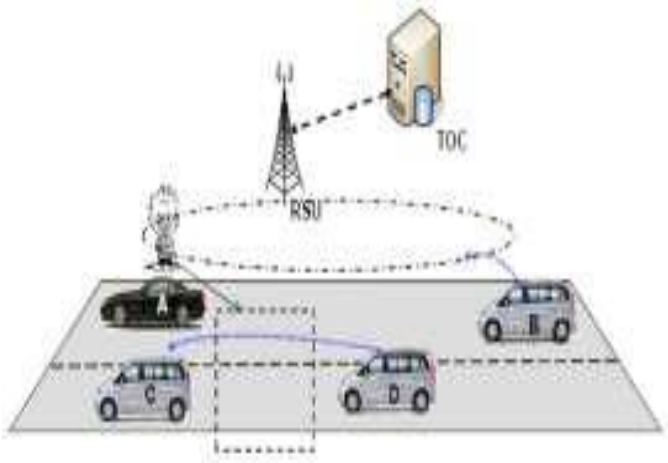

Fig. 2: Denial of Service (DOS) between V2V and V2I [2].

In this case the attacker A launches a DOS attack thus jamming the communication medium between V2V and V2I and denying B, C and D (Authentic Users) from communicating with each other.

III. PROPOSED PARTICLE SWAM OPTIMIZATION ALGORITHM

The Particle Swarm Optimization (PSO) algorithm is a population-based stochastic search algorithm. The PSO algorithm was first introduced by Dr. Kennedy and Dr. Eberhart in 1995. They were originally inspired by simulation of the social behavior of animals such as fish schooling and bird flocking. It attempts to mimic the natural process of group communication to share individual knowledge when such swarms flock, migrate or hunt. If one sees a desirable path to go, the rest of this swarm will follow. In PSO, the population is called a *swarm* while each member of the population is referred to as a *particle*. Each particle in the PSO has a randomized velocity associated to it, which moves through the space of the problem. Thus, in PSO the behavior of animals is limited by particles with certain positions and velocities in a searching space.

The implementation of PSO is as follows: Starting with a randomly initialized population and moving in randomly chosen directions, each particle 'flies' through the searching space while remembering the best positions it has seen. Members of particles of swam communicate good 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. As such, each particle makes its own decision and is influenced by its neighbor. Finally, all particles tend to fly towards better and better positions over the searching process until the swarm move to close to an optimum of the fitness. In PSO, each particle flies through the multidimensional space and adjusts its position in every step with its own experience and that of peers toward an optimum solution by the entire swarm. Thus, the particle follows three major principles: *evaluating* (learning through self experience), *comparing* (learning thorough comparative study), and *imitating* (learning through adapting the best trend). Therefore, the PSO algorithm is a member of Swarm Intelligence [5].

PSO shares many similarities with Genetic Algorithms (GA), which is one of the evolutionary computation techniques, except that PSO has no evolution operators (such as crossover and mutation) and does not implement the survival of the fittest individuals. Instead, PSO implements the simulation of behavior.

IV. SIMULATION RESULTS

Particle swarm optimization algorithm transitions particles in a probabilistic space using the velocity of the particle. This has implied that both the particle swarm optimization variables have a probability associated with them. The swarm tries to maximize the probability of a certain binary variable by having a velocity such that its probability is maximized. The algorithm uses the same velocity update equation as in (1) but the values of 'X' are now discrete and binary. For position update, first the velocity is transformed into an [0, 1] interval using the sigmoid function given by

$$S_{id} = sig(V_{id}) = \frac{1}{1+e^{-V_{id}}}$$

where, V_{id} is the velocity of the ith particle's dth dimension. A random number is generated using a uniform distribution which is compared to the value generated from the sigmoid function and a decision is made about the X_{id} in the following manner.

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

u is a unit step function. The decision regarding X_{id} is now probabilistic, implying that higher the value of the V_{id}, higher 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 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 particle swarm optimization, since particles do not get stuck once they find optima.

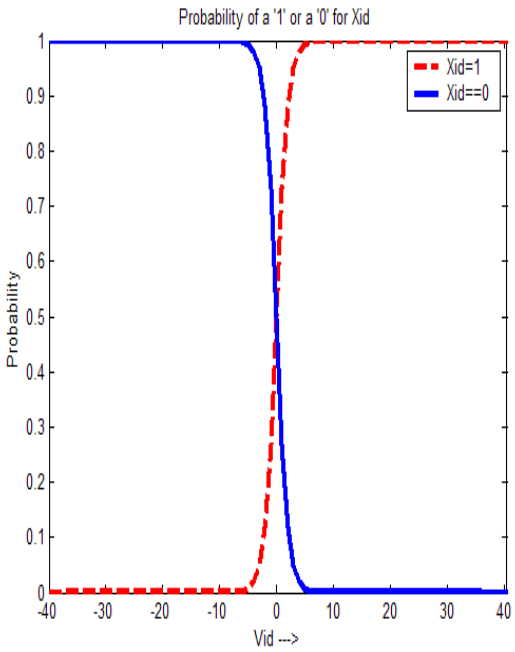

Fig. 3: Transformation of the Particle Velocity to a Binary Variable

Simulations were conducted on a Pentium 4, 3.2GHz computer, in the MATLAB R2011a environment. Two systems both PSO and GA were used for the identification task, the first given by:

$$G(s) = \frac{Ke^{-T_d s}}{T_2 s^2 + T_1 s + 1} = \frac{7.6e^{-25s}}{10s^2 + s + 1}$$

where the algorithms had to identify K, Td and T2 only. The second system was represented by:

$$G(s) = \frac{5.7e^{-42s}}{40.2s^2 + 4.2s + 1}$$

where the algorithms had to identify K, Td, T1 and T2. The proposed parameters were used to create a model output data set which was compared with the training data set (from the known parameters) using the Integral Absolute Error as the objective function to be minimized. For some tests, a perturbation has been added to the system response to represent noise (25% of the process signal), since real system measurements are rarely smooth. For both algorithms the population was set to 25 individuals, and a maximum generation of 100. The results of applying the genetic algorithm and particle swarm optimization to the identification problem are provided in Table 1. For each parameter the final value determined by the respective algorithm is given followed by its percentage difference from the actual value: for example for the first system, without noise, the particle swarm optimization determined T1 as 10.972, 9.72% above the actual value of 10.0. The second to last column presents the number of generations taken to arrive at the determined parameter value, while the final column reports the number of seconds required by the CPU for the complete simulation of 100 generations. In all cases the particle swarm optimization computation effort exceeds that of the genetic algorithm, ranging from 13% to 19% additional time required in comparison.

	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

Tabe 1: Results of applying the genetic algorithm and particle swarm optimization algorithm

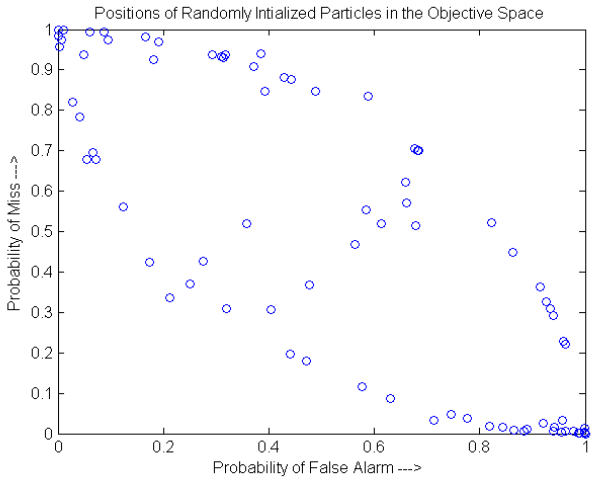

Fig. 4: Randomly initialized particles

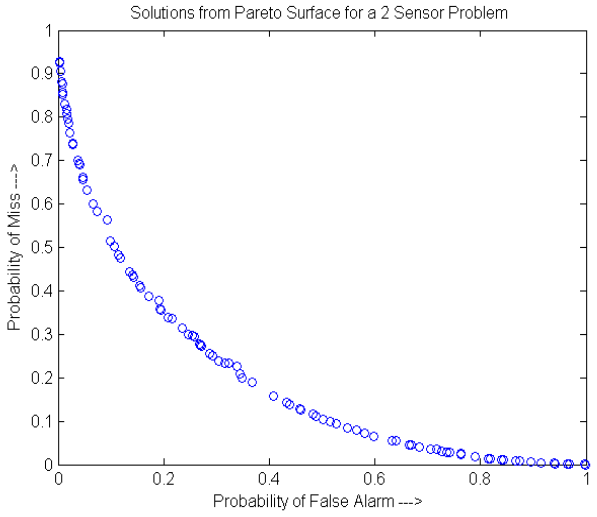

Fig. 5: Solutions from Pareto Surface for a 2 sensor Problem

ISSN: 2278 – 1323

IV. CONCLUSION

Denial of service attack is the most serious level attack in vehicular ad hoc networks such that the communication channel and network resources are unavailable to legitimate users. For preventing DOS attacks in VANETS a most reliable method of detection and prevention, Particle Swam Optimization (POS) is presented. The simulated results show that the proposed method is capable of detecting and preventing DOS attacks in VANETS.

REFERENCES

[1] 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
[2] Singh,S. and Parmar,U. (2015). Overview of various attacks in Vanets. *International Journal of Engineering Research and General Science*, 3(3), 120-125
[3] Willke, T.L., Tientrakool, P. and Maxemchuk, N.F (2009) A survey of inter-vehicle communication protocols and their applications. Communication Survey & Tutorials,11(2),3-20.
[4] Hasbullah,H., Soomro,I. A , Manan,J.A.(2010) Denial of Service (DOS) Attack and Its Possible Solutions in VANET,vol 4,pp 350-354
[5] M. Dorigo and M. Birattar (2007), "Swarm intelligence," in Scholarpedia, pp. 2(9):1462.

