International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 06, Issue: 06 (November- December, 2020)

# Artificial Swarm Algorithm Based Protection Scheme to Protect Network from Worm Hole and Black Hole Attack

**Sneha Hire, Shweta Sharma**
Computer Science and Engineering Department
Bhopal Institute of Technology and Science, Bhopal, India

**Abstract—** *Vehicle to Vehicle (V2V) Networks are an important part of Intelligent Transportation Systems (ITS). It is a network of moving vehicles that have their function to help make their way. Virtual Agents have attracted the attention of many researchers in recent years. This new technology enables value-added services such as road safety and managing traffic on the road. Security is a very important issue in this network of others. Wormhole and black hole attacks are very serious security dangers. A malicious node may provide fake routing information by advertising itself with the shortest path to the source node and then separating itself from the original route. This will cause the original path to switch, diverting forwarded nodes to the malicious node. In this thesis, we propose a Clustering-based intelligent water drop algorithm for attack detection in VANET communication. We thought of a system based on standing information-stations and vehicles that are usually moving. Vehicles share their cluster's primary responsibility for the next move or assign time. Much like water fountains in public malls, each vehicle in a cluster will communicate with its cluster head. The cluster head will detect an attack, and provide trusted routes for communication to the cluster nodes. Results from the simulation show that our approach is suited to the increasing use of vehicles, suggesting applicability with future vehicles.*

## I. INTRODUCTION

With the growth of wireless communication techniques, vehicular ad hoc networks have become a promising technology. It is expected to improve the efficiency and safety of the transportation system. Vehicular Ad hoc Network provides many facilities like traffic congestion control, passenger safety, location-based services [1], etc. In Vehicular Ad hoc Network, there are two different types of communication [2] as shown in Figure 1.

1. vehicle to vehicle communication.
2. Vehicle to RSU communication.

On a wireless network, an attacker(s) can attack an open network (of all those open for all to see). As one can see, the security of a VANET system is very important as it inherits many of the wireless network's security concerns [3]. Many security threats have been discovered and introduced by many researchers in VANET. Both wormhole [4] and blackhole attacks [4] are considered serious threats to early adopters and carriers of the underlying web-of-things safety net. When the attacker sends the message, via the source (victim) node, to the destination (victim) node that has the shortest path to the destination. Since the victim (sender) node sends all of its data to it, it destroys the data. It is an attack called the Black Hole attack.

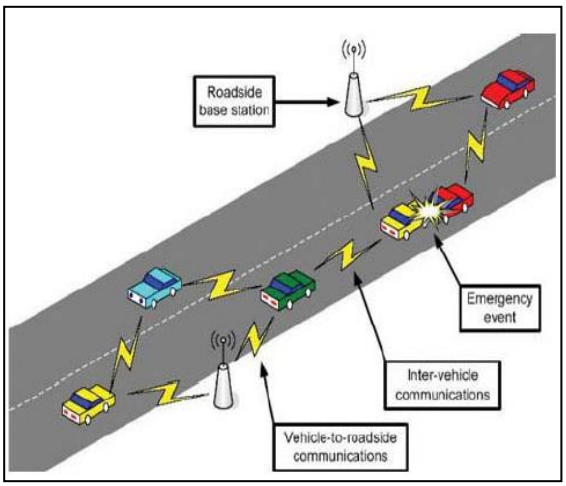


Figure 1 A simple schematic representation of a vehicular ad-hoc network.

On the other hand, if the attacker has successfully implemented a wormhole attack, it would also receive the data and send it to other attackers through the high-speed tunnel and use it across for its purpose. The Cloud computing strategy "Informatics will Defend the Earth" is implemented by a swarm of Artificial electric neurons inside the earth with an irregular shape, by which people look like to be more as "swarm" than "human" in the real world. This method has some perceived disadvantages; when traffic load is increased, the message's delay time is increased [5,6,7].

**IWD Artificial swarm algorithm:**

The application of swarm algorithms for constructing secure routes in peer-to-peer networks with dynamic self-organization allows increasing safety, much like an orderly swarm map-making, where the swarm is well structured and manages to recognise and continue picking the best routes. As another means of collecting vehicle data, the developed swarm algorithm allows the collection of data by introducing pheromone-based swarms and swarms known for being able to determine the state of a vehicle network node. The parameter that most focuses on the relationships between the nodes of a network are the nodes' trust. A density-based real-time probabilistic forwarding result could reveal the impact of traffic intensities on network performance. It is still an open issue of whether to use density or lifetime as the most influential parameter for deciding the threshold for forwarding probability determination. A realistic model of traffic taken into account may explore further the effect of traffic on network performance by considering the effects on the hidden

and exposed terminals. The proposed scheme prevents black hole and wormhole attacks through which such attacks can ward off. To reduce the risk of black holes and wormholes, we had to use clustering technology. To promote data transmission in the water, this droplet mechanism has been introduced. The rest of the paper is organised in the following order. The second section deals with the attacks in the "Visual Augmented Reality" network. Section three addresses the proposed prevention and detection system. The fourth section of this paper comprehensively evaluates the design and security of this proposed scheme.

## II. ATTACKS IN VANET

A. ***Denial of Service Attack:*** In a DOS (denial of service) attack, the objective is to prevent a legitimate user from accessing the resources and services he or she has the privilege to use. In such a scenario, it is possible that a vehicle has hijacked the entire network and is preventing healthy phones from doing anything productive. DOS attacks are a serious one in which users cannot communicate with the user due to a DOS attack. An attacker continuously makes a node overused in an under-performing manner to overwhelm the node and enable it to be too busy to perform the necessary tasks. It does packet dropping, rather than say, echoing around [8].

B. ***Distributed Denial of Service Attack:*** Distributed denial of service (DDoS) is more harmful than Distributed computing because it is distributed. The effects and motives of the attack depend on the different currents the attacker uses. E-mail messages might be sent at different times, possibly sending at a different time. Each vehicle would often send a message differently based on its time and location. DDOS is possible using V2V and V2I devices. Its main objective is to slow down the network and to jam the network [8].

C. ***GPS Spoofing:*** The database on the network will keep track of the vehicle's identity with its actual location. The enemy generates a GPS signal from a satellite to mess with the vehicle; this is more effective than the original signal.

D. ***Timing Attack:*** For a network's best to happen, there should be accuracy in the timing of when packets can arrive. This would help e-commerce. As a security measure, a timing attack can occur with ITS safety. In this attack, the attacker would add an extra piece of data to the original piece of data and modify it. Due to the absence of a special meter, messages take more of a long time on average to reach their destination. Its application must be efficient in terms of time, and it requires data to be transferred in time, else a serious accident may happen.[8].

E. ***Sybil Attack:*** The purpose of this is to send multiple messages from one node with multiple identities. Sybil attack is possible except in very narrow circumstances, such as when the set of involved entities is perfectly coordinated, and there are no privacy concerns. When there is a node that creates multiple copies of themselves, then the nodes become confused. Pick up all the illegal and fake IDs and security card and Authority. There can be a disclosure collision in the network [9]. This kind of attack is inherently difficult to imagine in the world of networks. This code can attack from both inside and outside the computer. Authentication will protect against external attacks but not against internal ones because there is a one-to-one mapping between the identity of the entity and the matching entity in the network.[10].

F. ***Grey Hole Attack:*** When a malicious node disrupts the flow of all the protocols it has to travel through, neighbouring nodes will easily spot it. Since the intruder can destroy the packets of data selectively, the rest of the broadcast should be received correctly.

G. ***Sinkhole Attack:*** A malicious network randomly chosen by a given routing algorithm could be the optimal choice for all surrounding nodes of the algorithm. An example of how the violating node can interpret a packet is by sending routing messages, convincing all neighbouring nodes that it is the best node for subsequent transmission of the packet to the base station. By doing this, he will become the centre of a network, and he will have the ability to collect all the packets from the nodes going to the base station. With this one, we further open up the door for many different attacks.

H. ***Wormhole Attack:*** A malicious vehicle intercepts data packets route, and delivers them to another malicious vehicle using a high-speed wormhole link (tunnel). Thus, a source to destination communication is achieved through these malicious vehicles. The impact of this attack is that it disrupts the discovery of valid routes and, in the process, potentially jeopardizes the security of data packets.

I. ***Black Hole Attack:*** A malicious node corrupts all packets it receives, causing errors for all packets they forward. The node plays a key role in identifying a collection point. The combination of these two factors may have disrupted the process of transmitting a huge amount of data.

## III. PROPOSED APPROACH

In a vehicle network, a Vehicle Node has to elect a Node Cluster Head Node, which can perform proper data publication and subscription operation on behalf of the initiator Node. This node is a final point in a network. Should another node be added to the cluster, this node becomes the final point in the cluster. This algorithm's communication strategy uses selective relaying scheduling for both the internal and external segment of communication. Regardless, communication with the cluster head is still the responsibility of the team member. The algorithm is completed as follows:

***Cluster Head Selection:*** The vehicle broadcasts out a packet composed of the vehicle speeds, last samplings were taken, and the last place the vehicle is linked. The vehicle receives a message (speed, last sampling location, and links are to the last station the vehicle passed). OBU counts the number of replies the post has received; these links are called connection links. While waiting for a bus, OBU collected packets of info about their bus stop. These can then be compared to a piece of information they already have, using information from the next array. Now, this "Array" uses this "Connecting Links" as inputs to produce an output. If values are sent to the next array, they'll be the same values as those values were again sent to the next array. This comparing concept relies on the speed at which OBU is turning if the speed of OBU is greater than the other one selected as cluster-head; otherwise, it will wait until the notification of the cluster-head. Assume that the first connecting section is "X", the speed of the vehicle is "Y", and the last information station is "Z". The algorithm to implement this process is as follows:

*Broadcast hello packets in the network (Speed, Last Info-station).*

***i)*** ***Put packet in a queue a [$Z_i$].***
***ii)*** ***if (Z = a [$Z_i$])***
***iii)*** ***Put packet in a queue b [$X_i$].***
***iv)*** ***if (X >= b [$X_i$])***
***v)*** ***if (X= b [$X_i$])***
***vi)*** ***Put above packet data in a queue c [$Y_i$]***
***vii)*** ***if (Y <= c [$Y_i$])***
***viii)*** ***Broadcast its address as Cluster Head.***
***ix)*** ***Else***
***x)*** ***Discard Packets.***
***xi)*** ***Else***
***xii)*** ***Wait for Cluster Head notification.***
***xiii)*** ***Else***
***xiv)*** ***Broadcast its address as Cluster Head.***
***xv)*** ***Else.***
***xvi)*** ***Wait for Cluster Head notification.***

Cluster Head Trust Calculation & Attack Detection Module:

***[i].*** ***Broadcast packet to each cluster node.***
***[ii].*** ***Cluster Head receives pheromones.***
***[iii].*** ***Entering pheromones values into the routing table.***
***[iv].*** ***Periodically collects information from the cluster nodes.***
***[v].*** ***Summing pheromone values from the routing table.***
***[vi].*** ***Calculation of the average value of pheromone per unit time.***
***[vii].*** ***Trust(t) = Trust (t-1) + w * $K_j$***
***[viii].*** ***(Where K = [delay, reply, bandwidth]***
***[ix].*** ***'w' is the weighting coefficient of the parameter, Kj is the parameter)***
***[x].*** ***Comparison with the threshold value.***
***[xi].*** ***If trust is less than the threshold value go to step ix.***
***[xii].*** ***Else go to step x***
***[xiii].*** ***Changing the status of a node to "insecure".***
***[xiv].*** ***Delete a route for this node.***
***[xv].*** ***Make that secure node enable.***
***[xvi].*** ***Saves the current node status.***
*[xvii].* ***End***

***Input Module:*** When an electronic ignition system comes to the onboard unit of a vehicle. It verifies the source address and that it matches the cluster head address. The control unit checks the packet: an update, a copy data, or a control information packet. The unit then forwards the packet based on which it is the control information packet if a true discard means the unit is not obligated to forward it because it is not the update packet, and then the unit fulfils the dissemination.

***i)*** ***Extract input data-id (vehicle id, control information, data)***
***ii)*** ***Match input data-id with cluster id.***
***iii)*** ***If (cluster id = input id)***
***iv)*** ***Discard related entry from regarding tables.***
***v)*** ***Else***
***vi)*** ***Put an entry in regarding the table.***

## IV. RESULTS

Many completely simulated experiments have been performed (simulator equals "running", used twice in a sentence). Table 5.1 shows the model parameters and the values for each parameter. To see how the proposed approach can operate under busy traffic conditions, it has been tested in a scenario of a rectangular area of 1,000 x 1,000 metres; the network topology consists of the different number of vehicle nodes. Two types of communication traffic are used in the NS2 simulation: CBR (Constant Bit Rate) traffic is used to generate UDP packets and FTP (File Transfer Protocol) traffic to send the data to the remote host. During input, the time is set from 0ms to 300ms. After the time has been entered, the Sybil detection algorithm will start from 0.001ms and check at 0.5ms. Different packets sizes are used in the NS-2, for this simulation 1024KB packets are used.
There are four-way highways, and they have two parallel lines in each direction on them. There are also four different cross-over locations for vehicles to and from each other to travel across. Because we assume that the exit vehicles will be the ones sending notices to the vehicles on the highway, we "assume" that they will enter the highway at the closest highway end and immediately send messages. We have selected a single vehicle as to the attacker, and remaining are normal vehicle node. A simulation of the proposed algorithm has been run to examine the performance of the

algorithm's outcomes. Each car is spread out onto separate locations on one street. We'll have a few people mix/different match paths. Each vehicle in the experiment is driven at a randomly fluctuating speed on different streets. Wireless communication parameters are listed in Table 1. Performance of our approach is measured based on packet delivery ratio, end to end delivery. There are two different approaches for which we measure packet delivery ratio. Those two approaches are 1) IWD Artificial swarm algorithm, 2) Cluster Based IWD Artificial swarm algorithm. Simulation graphs are as follows:

Table 1 Simulation Parameters

| Parameter | Default Value |
|---|---|
| Simulation Area | 1000m * 1000m |
| Simulation Time | 300 minutes |
| Number of vehicles | 60 |
| Communication range | 400m |
| Node Speed | 60km/hr |
| Visualization Tool | NAM |
| MAC layer | IEEE 802.11 p |

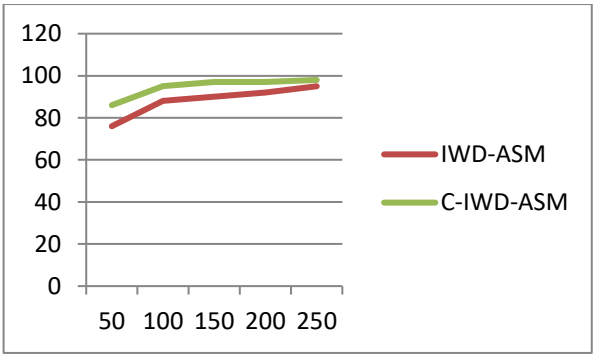


Figure 2 Graph-Packet delivery ratio of "IWD-ASM" & "C-IWD-ASM."

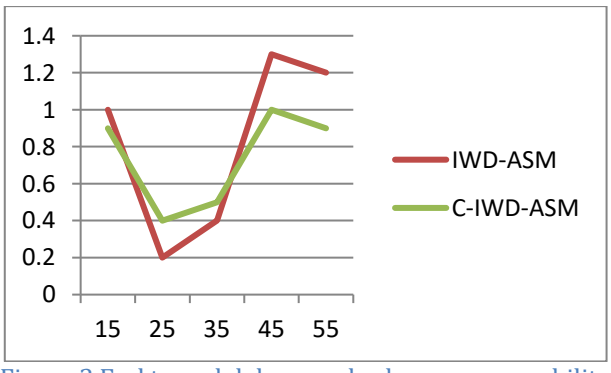


Figure 3 End to end delay graph, shows comparability of "IWD-ASM" & "C-IWD-ASM."

## CONCLUSION

We have proposed a hybrid technique for black hole and wormhole attack detection, which automatically identifies when a black hole and wormhole attack is detected. Our secure route application is a quick demonstration of how peer-to-peer networks can automatically detect black hole and wormhole attacks. By taking advantage of modern technologies, we developed a swarm computing algorithm that allows us to quickly and efficiently collect information from a large network within a given amount of time and without compromising efficiency in networking or lowering the network's delay time. This method employs on each vehicle's on-board unit (OBU), in which OBU elect their cluster head and then only communicate with cluster head or info-stations. Communication paradigm, which is used in our approach is systematic scheduling. The technique is localized, requires only a small overhead, and does not have special requirements such as special hardware etc. For dynamic connectivity methods, the technique was tested on various types and distributions of clusters. Under all the evaluated scenarios, the technique is excellent at spreading the disease. The results of the guidance that we produced are more expensive than the previous strategies to reduce the cost of routing packets and reduce the delay time, decreasing the network's cost.

## REFERENCES

[1]. Alimohammadi M., Pouyan A. A.; Vehicular Ad Hoc Networks: Introduction and a proposal for vehicle positioning; 13th International conference on Traffic and Transportation Engineering; 2014.

[2]. Douceur J. The Sybil attacks. Proc. of International Workshop on Peer to-Peer Systems 2002; 251– 260.

[3]. Isaac, J. T., Zeadally, S., & Camara, J. S. Security attacks and solutions for vehicular ad hoc networks. Communications IET 2010; 4(7): 894

[4]. Alimohammadi M., Pouyan A. A.; Defence Mechanisms against Sybil Attack in Vehicular Ad hoc Network, Security and Communication Networks, John Wiley & Sons, 2014.

[5]. V. Krundyshev, M. Kalinin and P. Zegzhda, "Artificial swarm algorithm for VANET protection against routing attacks," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, 2018, pp. 795-800.

[6]. Xiao, B., Yu, B., & Gao, C. Detection and localization of Sybil nodes in VANETs. Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks 2006; 1-8.

[7]. Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. Lightweight Sybil Attack Detection in MANETs. IEEE, Systems Journal 2013; 7(2):36- 248.

[8]. Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks.

Selected Areas in Communications, IEEE Journal 2011; 29(3): 582- 594.

[9]. Jaydeep P. Kateshiya and Anup Prakash Singh," Review to Detect and Isolate Malicious Vehicle in VANET", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 2, February 2015, pp: 127-132.

[10]. Komal Rani and Meenakshi," Prevention of Denial-of-Service Attack on Dynamic Source Routing VANET Protocol", IJRET: International Journal of Research in Engineering and Technology, Volume: 04 Issue: 09 | September2015, pp: 251-255.

[11]. E. Ngai, L. Jiangchuan, and M. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," IEEE International Conference on Communications, 2006, vol. 8, pp. 3383-3389.