International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 06, Issue: 01 (January- February, 2020)

Clustering Based Intelligent Water Drop Algorithm (CIWD) To Protect Against Multiple Attacks in Vehicular Ad Hoc Network

Rahul Patidar, Vimal Tiwari
Department of computer science and engineering
Bhopal Institute of Technology & Science
Bhopal, M.P., India

Abstract— *Vehicular Ad-hoc Networks (VANET) is an important component of Intelligent Transportation Systems. It can be envisaged as the network of moving vehicles communicating autonomously and unevenly. VANET has attracted the attention of many researchers in recent years. It enables value-added services such as road safety and m`anaging traffic on the road. Security issues are challenging problems in this network. Wormhole and Blackhole attacks are very serious security threats in which a malicious node provides fake routing information by advertising itself having the shortest path to the source node and then deprive the traffic of the source node or can drop the packets later. In this thesis, we propose our Clustering-based intelligent water drop algorithm for attack detection in VANET. In our approach, we assumed a hybrid VANET consisting of stationary info-stations and moving vehicles, where vehicles elect their cluster head which is responsible for their further communication, each vehicle in a cluster will communicate with cluster head and cluster head will detect the attack in-network and provide trusted routes for communication to its cluster nodes. Simulation results show that our approach performs well with the increasing number of vehicles which suggests the applicability of our approach.*

I Introduction

Day by day increasing the reliability and dependence on wireless communication techniques, Vehicular Ad hoc Network has become a promising technology. It has the potential to improve the efficiency and safety level of the transportation system. Vehicular Ad hoc Network provides many facilities like traffic congestion control, the safety of passengers and vehicles, location-based services [1], etc. In Vehicular Ad hoc Network, there are two types of communication [2] one is Vehicle to vehicle communication and another one is Vehicle to RSU communication shown in figure 1. Being a wireless network, the network is open for all, this leads to the danger of malicious attacker attacks on the network, and thus the security of VANET is a major concern as it inherits all the security threats of the wireless network [3]. A lot of security threats have been discovered and introduced by many researchers in VANET. One of these threats, wormhole and black hole attacks [4] are a serious threat to VANET security. In these attacks, the attacker sends a message to the source (victim node) that, it has the shortest path to the destination. Hence the victim node sends all data to it and it will destroy it.

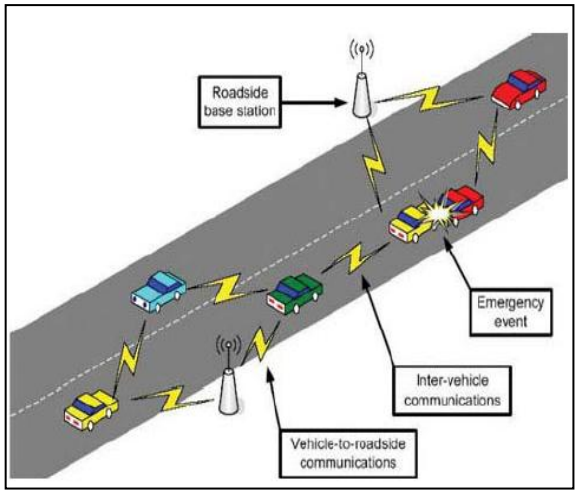

Figure 1 Schematic Representation of a Vehicular Ad-hoc Network

This attack is called the Black Hole attack. On the other hand, if the attackers implementing a wormhole attack, it receives the data and sends this data to another attacker through the high-speed tunnel and uses this data for his purpose. For mitigating these attack different methods were implemented by researchers, IWD Artificial swarm algorithm (Intelligent Water Drop) [5, 6, 7] is one of them, this method has some disadvantage, due to this when traffic load is increased, the delay time is increased as well.

CIWD Artificial swarm algorithm:

Application of swarm algorithms for constructing secure routes in peer-to-peer networks with dynamic self-organization allows increasing the level of safety, at the same time, thanks to the realized dynamic decision to build routes; network characteristics became a bit more progressive. The developed swarm algorithm allows us to quickly collect data on the status of vehicular network nodes through the introduction of pheromones and the use of agents collecting information about the availability of the node. The most important parameter characterizing the relationship between the nodes of the network is the trust of the nodes to each other. . Density-based probabilistic forwarding could reveal the impact of traffic intensity on network performance. How-ever, how to intelligently decide the threshold of density for forwarding probability determination is still an open issue. A realistic interference model may further explore the influence of traffic intensity on the network performance, with the hidden and exposed terminals considered.

The proposed scheme is a way to protect against black hole and wormhole attack respectively. To reduce the risk of Black and wormhole, we used the clustering concept. To regulate data dissemination intelligent water drop mechanisms has introduced. The rest of the paper is organized as follows. Section II describes the attacks in VANET Section III presents the proposed prevention and detection scheme. Section IV evaluates the performance and security related issues in the proposed scheme.

II Attacks in VANET

A. Denial of Service Attack: In DOS attack the main objective is to prevent a legitimate user from accessing resources and services. This attack can be trigger by jamming the whole channel and network so that no authorized vehicle can access the network. It is a serious problem in which the user is unable to communicate with the user due to the DOS attack. At the basic level, the attacker forces node and make it busy to do unnecessary tasks by overwhelming it so that it could not do necessary tasks. So it is responsible for packet dropping [8].

B. Distributed Denial of Service Attack: DDOS is more harmful than a DOS attack because it is in a distributed manner. Different types of locations are used by the attacker to launch the attack. It might be possible that they use different time slots for sending messages. The nature of the message and time slot varied from vehicle to vehicle. DDOS is possible at V2V and V2 I. Its main objective is to slow down the network and jam the network [8].

C. GPS Spoofing: The table is maintained in the network to update all the information regarding the identity of the vehicle and the geographic location of the vehicle. The attacker generates GPS satellite signals to fool vehicles which are more effective than the original signals.

D. Timing Attack: There should be accuracy in the time for the best performance of the network so the delay should be less in any application. A timing attack is an issue in ITS safety applications. In this attack, the attacker instead of modifying the data; adds more content in the original data. Due to addition message takes more slot to reach to the destination rather than the required time. So ITS application is a crucial application which is dependent on time and it requires data transmission on time otherwise serious accident may happen [8].

E. Sybil Attack: It consists of sending multiple messages from one node with multiple identities. Sybil attack is always possible except for the extreme conditions and assumptions of the possibility of resource parity and coordination among entities. When any node creates multiple copies of itself then it creates confusion in the network. Claim all the illegal and fake ID and Authority. It can create a collision in the network [9]. This type of situation is known as the Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in the network [10].

F. Grey Hole Attack: When a malicious node destroys all received packets, it can be easily detected by neighboring nodes. Therefore, the intruder can destroy data packets selectively, and the rest can be broadcast correctly.

G. Sinkhole Attack: A malicious node can be the most optimal for all surrounding nodes from the routing algorithm [11]. For example, the violating node can send out routing messages, convincing all neighboring nodes that it is the best node for subsequent transmission of the packet to the base station. This allows him to become a hub and collect all the packets from every node of his neighborhood going to the base station. This opens up great opportunities for subsequent types of attacks.

H. Wormhole Attack: A malicious vehicle receives the data packets at a point in the network and replays them to another malicious vehicle by using a wormhole high-speed link (tunnel) and hence a source to destination communication proceeds through these malicious vehicles. The impact of this attack is that it prevents the discovery of valid routes and threatens the security of transmitting data packets.

I. Black Hole Attack: A malicious node can destroy all the packets that it receives for subsequent transmission. This type of attack is especially effective when the node is also a collection point. This combination may be the reason for stopping the transfer of a large amount of data.

III Proposed Approach

The vehicle node in a network has to elect the cluster head node, which can do proper publication and subscription operation on the behalf of the initiator node. This cluster head is an ultimate place holder in the cluster for other nodes. The type of communication strategy used in this algorithm is selective relay scheduling for both internal as well as external, but communication responsibility is all in the shoulder of the cluster head. An algorithm is as follows:

Cluster Head Selection: For finding the cluster head, the vehicle sends a hello packet containing (Speed, Last Info-station Passed, and Connecting Link) in the network at a regular time interval and wait for its reply. When the reply comes, OBU counts the number of replies; these replies are referred to as connection links. These packets were collected in a queue where OBU compare them with its last info-station information if information matched send information into the next array. Now this OBU compare this array

with its connecting links; after comparing if two or more values are same than those values are again sent to the next array and this time comparison employed based on their speed if speed of OBU is greater than another one it is selected as cluster head else it will wait for cluster head notification. Assume connecting link of the vehicle is "X", speed of the vehicle is "Y", last info station is "Z". Algorithm for the above process as follows:

I. *Broadcast hello packets in the network (Speed, Last Info-station).*
II. *Put packet in a queue a [Z_i].*
III. *if (Z = a [Z_i])*
IV. *Put packet in a queue b [X_i].*
V. *if (X >= b [X_i])*
VI. *if (X= b [X_i])*
VII. *Put above packet data in a queue c [Y_i]*
VIII. *if (Y <= c [Y_i])*
IX. *Broadcast its address as Cluster Head.*
X. *Else*
XI. *Discard Packets.*
XII. *Else*
XIII. *Wait for Cluster Head notification.*
XIV. *Else*
XV. *Broadcast its address as Cluster Head.*
XVI. *Else.*
XVII. *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.*
    a. ***Trust (t) = Trust (t-1) + w * K_j***
    b. *(Where K = [delay, reply, bandwidth]*
    c. *'**w**' is the weighting coefficient of the parameter, Kj is the parameter)*
VII. *Comparison with the threshold value.*
    a. *If trust is less than the threshold value goto step ix.*
VIII. *Else go to step x*
IX. *Changing the status of the node to "insecure".*
X. *Delete a route for this node.*
XI. *Change node to "secure".*
XII. *Saves the current node status.*
XIII. *End*

Input Module: When any data packet comes to onboard unit of vehicle it checks its source address if this address is same as the cluster head address then onboard unit check what kind of packet is it control information packet, forwarding or data packet for itself and match this data with its tables if value is true discard regarding entry from table else follow regarding procedure for 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

To validate the proposed approach several simulation experiments have been performed by using network simulator version 2.34. Table 5.1 shows the parameters used in the simulation experiments. The proposed approach is tested in busy traffic conditions using a rectangular scenario of 1000 × 1000 m square area; the network topology consists of the different number of vehicle nodes. There are two types of communication traffic are used in the NS2 (CBR and FTP), CBR (Constant Bit Rate) traffic is used to generate UDP packets for the simulation. In the simulation, start on 0ms and end on the 300ms. The Sybil detection algorithm will start at 0.001ms in the simulation and recheck on 0.5ms. There are different packets sizes are used in the NS-2, for this simulation 1024KB packets are used.

able 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

There are four-way highways and they have two lines each direction. There are four crossings through which vehicles may cross each other on the highway. To have a fixed number of vehicles in the simulation, assume that the exit vehicles will enter the highway at the nearest highway end and immediately start to send messages. We have selected a single vehicle as to the attacker and remaining are normal vehicle nodes. A simulation has been carried out to evaluate the performance of the proposed method. Each vehicle is first randomly scattered on one intersection along the paths. Each vehicle is driven at a randomly fluctuating speed along different streets. Simulation parameters are listed in Table 1.The performance of our approach is measured based on packet delivery ratio, end to end delivery. There are two different approaches for which we measure the packet delivery ratio. Those two approaches are 1) IWD Artificial swarm algorithm, 2) Cluster Based IWD Artificial swarm algorithm. Simulation graphs are as follows:

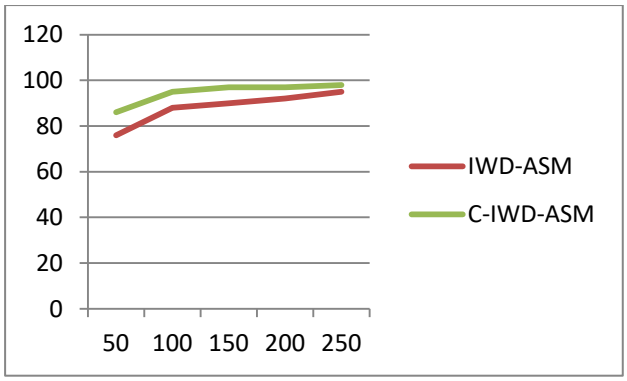

Figure 2 Graph-Packet delivery ratios of "IWD-ASM" & "C-IWD-ASM"

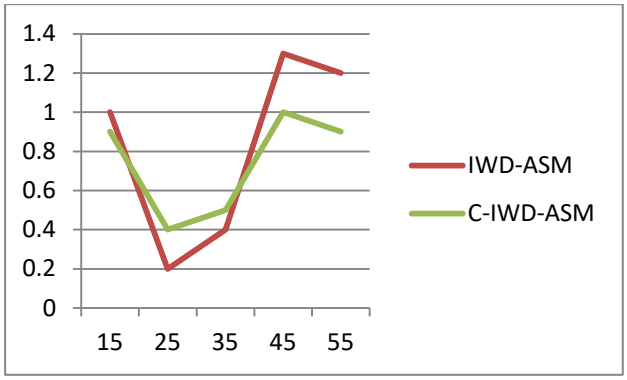

Figure 3 End to end delay graph, shows comparability of "IWD-ASM" & "C-IWD-ASM"

V Conclusion

We have proposed a hybrid technique for black hole and wormhole attack detection and presenting an application of swarm algorithms for constructing secure routes in peer-to-peer networks with dynamic self-organization allows increasing the level of safety. The developed swarm algorithm allows us to quickly collect data on the status by which any information in a network shall be spread in a network without increasing a routing load in a network as well as without compromises with 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. The 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. The technique was tested through simulations for different distributions of vehicles in dynamic connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent dissemination. The results of the proposed approach are battered than the previous approaches to reduce routing load as well as decreasing a delay time of a packet in a network.

Reference

[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 attack. 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.; Defense 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 AnupPrakash 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 Routingvanet 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.