International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 6
ISSN: 2454-4248
91 – 94

A Framework for Detecting Malicious Node in VANET

Prof. Vishal Shrivatava
M.Tech. Coordinator.,
Department of CSE,
Arya College of Engineering & IT

Ajay Samota
M.Tech. Scholar,
Department of CSE,
Arya College of Engineering & IT

Abstract: Vehicular ad hoc network (VANET) is a vehicle to vehicle (VVC) and roadside to vehicle (RVC) communication system. The technology in VANET incorporates WLAN and Ad Hoc networks to achieve the regular connectivity. The ad hoc network is brought forth with the objectives of providing safety and comfort related services to vehicle owners. Collision warning, traffic congestion warning, lane-change warning, road blockade alarm (due to construction works etc.) are among the major safety related services addressed by VANET. In the other category of comfort related services, vehicle users are equipped with Internet and Multimedia connectivity. The major research challenges in the area lies in design of routing protocol, data sharing, security and privacy, network formation etc. We aim here to study the overview of VANET and its security issues.

Keywords— *Vehicular Ad hoc networks, VVC, routing protocols, security and privacy.*

******

I INTRODUCTION

Vehicular Ad-Hoc network is a type of MANET, to give correspondence among near to vehicles and amongst vehicles and nearby fixed equipment i.e. roadside equipment. VANET or Intelligent Vehicular Ad-Hoc Networking gives a clever method for utilizing vehicular Networking. Every vehicle outfitted with VANET device will be a node in the Ad-hoc network and can get and transfer different messages through the wireless network [1].

II COMPONENTS OF VANET

VANET is a self-governing self-sorting out wireless network. VANETs contains taking after elements:

a) **Vehicles**: Vehicles are the nodes of vehicular network.
VANET handle the wireless discussion between vehicles (V2V) and amongst vehicles and base access point (V2I).

b) **Infrastructure:** Infrastructure identified with outside condition incorporate road side base station. Base stations are the roadside unit and they're placed at dedicated place like junctions or near parking areas. Their foremost features are to broaden the communication field of the ad hoc network with the aid of re-allocating the understanding to others and to run security utility like low extension cautioning, mishap cautioning and numerous others.

c) **Communication channels***:* Radio waves are a kind of electromagnetic radiation with wavelengths in the electromagnetic range longer than infrared delicate Radio waves have frequencies from 190 GHz to 3Khz. Radio proliferation demonstrate assumes a solid part in the execution of a protocol to decide the quantity of nodes inside one collision space [2].

III CHARACTERISTICS OF VANET

Vehicular network have some unique sort of conduct and characteristics, which distinguishing them from other types of network. As contrast with different networks vehicular network have remarkable and interesting features as follow:

a) Unlimited Transmission Power
b) Computational capacity very high.
c) Predictable mobility
d) High mobility
e) Partitioned network
f) Network topology and connectivity

IV SECURITY IN VANET

Security in VANET ought to be considered as vital as securing different networks in registering. Because of the profoundly delicate nature of data being communicated through VANET, all applications intended for vehicular network should be shielded from malicious manipulation. Imagine the likelihood of a basic message been manipulated and the harm it will cause if not detected. Notwithstanding that, comfort and quality applications in VANET need to be protected to prevent loss of revenue. [3] In the event that one applies this model of security at vehicular network, the one risk that truly emerges is the *confidentiality* of the source. For instance, an attacker who is occupied in breaking down, which authentications are appended to every message disseminated in the framework, may likewise have the capacity to track the precise area of the vehicle (trade off of protection). An inside attacker can make bogus safety messages to be distributed in the entire network. This can

 ISSN: 2454-4248
91 – 94

cause disastrous situations (a threat to Authenticity).ID Disclosure Location information in relation to vehicle exact position (privacy) needs to be protected (a threat to Confidentiality).

Denial of Service Attackers can potentially flood the entire network so that no one will have the capacity to utilize the applications/services. Such conditions can make terrible situations if activated immediately (a risk to Availability). The two key challenges in connection to giving a protected correspondence in VANET can be briefly classified as establishing a robust system of sender authentication and providing a mechanism to keep the user location undisclosed.

V MOTIVATION

In existing Malicious and Irrelevant Packet Detection Algorithm malicious node is detected on the basis of node speed. In existing work frequency of packet generation depend on node's maximum speed but it is not the correct way to find out malicious node in VANET because it is not necessary that node which is highly movable will behave like malicious.

VI RESEARCH OBJECTIVES

VANET communicates wirelessly which make them vulnerable to attacks like DoS Attack which essentially hinders the services and users are not ready to utilize the administrations. Proposed work aims to -

i. Calculate the speed of vehicles and how frequent a vehicle changes its speed.

ii. After speed calculation we check behavior of vehicles so that we can recognize the true malicious nodes in network scenario.

VII PROPOSED METHOD

Vehicular ad-hoc network is a standout amongst the most intriguing regions of research as a result of its foundation or high moveable. There are number of problems to build this network due its heterogeneous behavior. This network easily threaten by attacks, so in this case how to preserve network by attacks is difficult to understand there are lots of technique present to detect or prevent this network by attacks. Preventing network by this attack proposed approach apply speed and deportment based broadcasting path for VANET. In first phase it calculate the speed of vehicles and how frequent a vehicles change its speed, then after speed calculation it checks deportment of vehicles so that one can recognize the true malicious nodes in network scenario.

VIII PROPOSED ALGORITHM

Step1: Initialize vehicle network
Step2: Calculate Vehicle speed
Step3: If (Speed >=gateway)
{
Vehicle node dose not forward data
Else
V2V/V2I communication

Step4: If (Vehicle speed change frequency)
{
Use Trusty function ()
Else
Normal execution

Step5: If (Trusty >= gateway)
{ Normal nodes communication
Else

Malicious node
Trusty function ()

Step6: Exit.

Trusty function:

Trusty function work for finding malicious nodes in VANET scenario

Step1: If (drop packet is true) {
Trusty —
If (communication breaks)
{
Trusty – }
Else
Unchanged}
Else
Unchanged
Step2: Exit.

IX EXPERIMENTAL ENVIRONMENT

The simulation of our work done on NS-2.35 taking following parameters for network simulation which is required by our scenario. The table 1 shows the various parameters used and their **values.**

TABLE 1 :GENERAL PARAMETERS OF EXPERIMENT

Parameters	**Values**
Tool	Ns-2.35
Protocol	AODV
Antenna	Omni-directional
Number of Nodes	30
Simulation Time	100ms
Data rate	CBR
Buffer type	DropTail

 ISSN: 2454-4248
91 – 94

V. RESULTS

(i) Packet Delivery Ratio (PDR):
It outlines the proportion of packets deliver from supply toward to destination. PDR show the ratio between the packets received as compared to the packets sent in the network.
PDR = No. of packets received / No. of packets sent

TABLE 2: PACKET DELIVERY RATIO

Time (ms)	Reference Approach	Proposed Approach	% improvement
10	64.3157	87.7033	36.36
20	65.2092	88.9217	36.36
30	65.4503	89.2504	36.36
40	65.5237	89.3506	36.36
50	65.6204	89.4824	36.36

Table 2 shows the resultant values of Packet Delivery Ratio at different intervals of time for both previous base approach and proposed approach.
The fig. 1 shows a graph comparing PDR values for both previous base approach and proposed approach. There is x-axis and y-axis in the graph in which x-axis show the time of simulation for the overall network and y-axis show the PDR value at each interval of time. This PDR rate is better in proposed than existing approach. It shows an average improvement of 36.36% in comparison to previous approach.

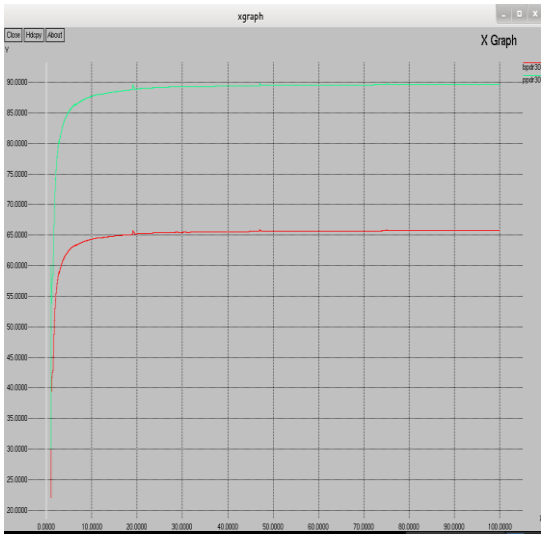

Figure 1. Comparing PDR of Previous and Proposed Approach

(ii) Throughput:
The transfer of information lying on information measure is decision as output. Throughput should be greater for the arrival of packets for the particular duration of time.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

Time (ms)	Reference Approach	Proposed Approach	% improvement
10	729.96	995.4	36.36
20	778.837	1062.05	36.36
30	794.334	1083.18	36.36
40	802.248	1093.97	36.36
50	806.799	1100.18	36.34

TABLE 3:

THROUGHPUT

Table 3 shows the resultant values of Throughput at different intervals of time for both previous base approach and proposed approach.

The fig. 2 represents an output graph among previous base approach and projected approach. There is x- axis and y-axis in the graph in which x-axis show the time of simulation for the overall network and y-axis show the throughput value at each interval of time. The output of the projected approach is enhanced than the previous approach. It shows an average improvement of 36.35% in comparison to previous approach.

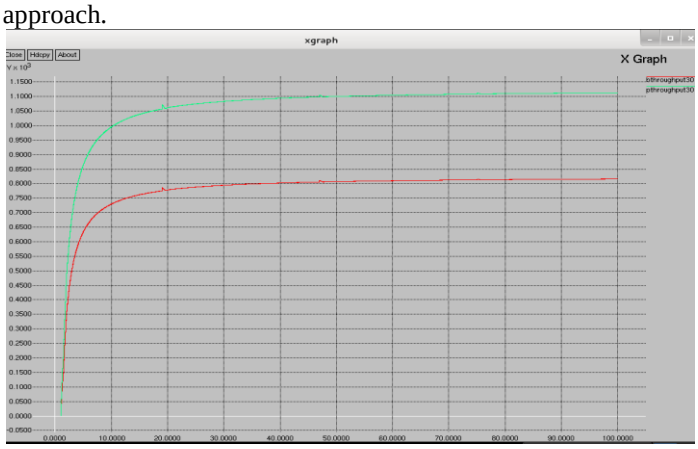

Figure 2: Comparing Throughput of Previous and Proposed Approach

(iii) Routing Overhead:
It is characterized as the aggregate number of packets required in the network. Routing overhead should be less for the better efficiency of the network which shows that there are fewer packets for the communication.
Routing overhead = Number of packets control in particular time.

 ISSN: 2454-4248
91 – 94

TABLE 4: ROUTING OVERHEAD

Time (ms)	Reference Approach	Proposed Approach	% reduction
5	604.636	443.4	26.66
10	1372.59	1006.57	26.66
15	2140.55	1569.73	26.66
20	2910.5	2134.37	26.66
25	3677.55	2696.87	26.66

Table.4 shows the resultant values of Routing Overhead at different intervals of time for both previous base approach and proposed approach.

The fig.3 represents a routing overhead graph among base approach and proposed approach. There is x- axis and y-axis in the graph in which x-axis show the time of simulation for the overall network and y-axis show the routing overhead value at each interval of time. The proposed approach has an extra overhead than the base approach. Since the overhead be supposed to be minimum except as the routing increases in the proposed work the overhead also increases.

It shows an average improvement of 26.66% in comparison to previous approach.

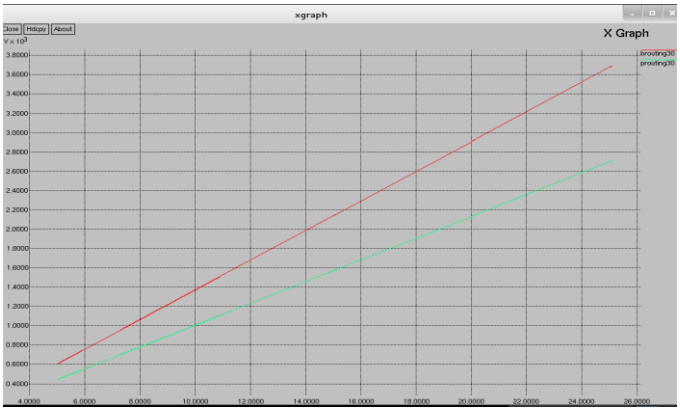

Figure 3: Comparing Routing Overhead of Previous and Proposed

Approach

X RESULT ANALYSIS

From table 2 to 4 and from fig. 1 to 3, it is clear that the proposed approach is better than previous approach. It shows an average improvement of 36.36% in packet delivery ratio and an average improvement of 36.35% in throughput in comparison to previous approach. It also shows 26.66% reduction in packet overhead in comparison to previous approach.

XI CONCLUSION

Wireless Ad Hoc Network (WANET) is ad hoc network in which nodes openly communicate and they act as a node or a router which construct them less dependent on each other. Mobile ad hoc networks (MANETs) are susceptible to various security attacks conducted by the malicious nodes and attackers. VANET is the wireless network in which correspondence happens through wireless links mounted on every moving node (vehicle). Every node inside VANET go about as both, the member and router of the network as the nodes communicate through other intermediate node that exists in their own transmission extend. Vehicular ad-hoc network is a standout amongst the most intriguing regions of research as a result of its demand or high usage. There are number of problems to build this network due its heterogeneous behavior. In our proposed work, we improved various qualities of services in the network like throughput, routing overhead and packet delivery ratio. Security is also improved by detecting and eliminating malicious nodes from the network.

REFERENCES

[1]. Sameena Naaz **“** Routing in Vehicular Ad Hoc Network (VANET)**”** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, December 2014.

[2].] Divya Chadha, Reena, **“**Vehicular Ad hoc Network (VANETs): A Review**”**, IJIRCCE, 2015.

[3]. C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, **“**A routing strategy for vehicular ad hoc net-works in city environments,**”** IEEE Symposium Proceedings on Intelligent Vehicles, pp. 156–161,2003.

[4]. Frank Karg, Zhendong Ma, and Elmar Schoch, “Security Engineering for VANETs” In 4th Workshop on Embedded Security in Cars (ESCAR 2006), Berlin, Germany, 11/2006.

[5]. Aijaz, B. Bochow, F. D¨otzer, A. Festag, M. Gerlach, R. Kroh and T. Leinm¨uller, **“**Attacks on Inter Vehicle Communication Systems – an Analysis,**”** The Network on Wheels Project, Tech. Rep., 2005. Available: http://www.network-on- wheels.de/documents.html.