THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Simulation Framework for Traffic Control, Secured Communication & Privacy Protection with Intrusion Detection for VANETs

Nandini Patil
Professor, Godutai Engineering College for Women, Karnataka, India
Ashwini
Student, Godutai Engineering College for Women, Karnataka, India
Kayadhu
Student, Godutai Engineering College for Women, Karnataka, India
Mukta
Student, Godutai Engineering College for Women, Karnataka, India
Shruti Y.
Student, Godutai Engineering College for Women, Karnataka, India

Abstract:
VANET architecture supports the inter-vehicular communication as well as vehicle to infrastructure communication by means of the direction of the vehicles, mitigation of the events such as accidents, bad roads are being propagated. However, increasing usage of VANETs has resulted in security concerns, such as eavesdropping (unwanted vehicular information been obtained by unauthorized nodes), privacy hacking (obtaining the data of the government vehicles and other important vehicles) miss information (vehicles mitigating false alarm about an accident or congestion in a part of a road). Therefore, VANET requires updated support for intrusion detection system, intrusion mitigation and risk minimization of the system.
our study finds out that such a V2V communication adds immense amount of overheads and is not realistic for intrusion detection as well as for mitigating the event notification. Therefore, in this work we have proposed a noble V2I configuration for intrusion detection system where the intrusion detection is being performed by the infrastructure known as RSU, from the information obtained by the vehicles. We show through the results, that our proposed system produces the better packet delivery ratio at a lower latency with an improved accuracy for intrusion detection system over conventional V2I system.

Keywords: *Ad hoc networks, inter-vehicular communication, navigation, secure & privacy, vehicle-to-infrastructure communication, intrusion detection.*

1. Introduction

Vehicular Ad Hoc Networks (VANETs) are the spontaneous creation of a wireless network for data exchange - to the domain of vehicles. This scheme utilizes the online road information collected by a VANET to guide the drivers to desired destinations in a real-time. VANETs support a wide range of applications - from simple one hop information dissemination of, e.g., cooperative awareness messages (CAMs) to multi-hop dissemination of messages over vast distances. Vehicular Ad hoc Networks (VANETs) are the promising approach to provide safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system.

2. Present System

The past techniques are based on V2V (Vehicle-to-Vehicle) communication system, where vehicles coordinate among themselves about the information being generated and by this they are able to detect an intruding or misbehaving nodes.

3. Proposed System

In this work we have proposed a noble system, a V2I (Vehicle-to-Infrastructure) system combined with V2V (Vehicle-to-Vehicle) system. Whereby, RSUs monitors the events being generated by the vehicle and performs a statically analysis on the event to find out if certain messages are completely deviated from the messages being generated by the other nodes or not. Based upon such deviations the RSUs calculate the probable intrusion and that intrusion data is further mitigated amongst the other vehicles such that all other vehicles would block the vehicle which is generating such attack. The proposed system is simulated through VanetSim or JAVA based simulator and we have shown that our proposed model obtains better results in terms of not only detecting the intrusion but also at the same time ensuring better delivery of both event messages as well as GPS information being dissipated by the vehicles.

4. Problem Definition

1. Generally city traffic is managed through traffic lights which are generally managed through static timers however in a modern city scenario such timing based traffic lights do not work well.
2. The Information about the congestion in a part of a road, accidents in a part of road, road being damaged, road side work being going or a part of a road is quite difficult o mitigates among the vehicles most of the modern navigation services such as Google maps not real time enough to provide the drivers such information therefore often or not the drivers keep driving in a congested roads causing more congestion in the city traffic. This can be avoided if we can achieve a VANET where a vehicle can mitigate the information among each other and notify each other about the probable events in the road. however such kind of communication is uncontrolled which means that vehicle generally uses free Wi-Fi band or free wireless channel to mitigate the data. Such kind of communications are less secure therefore such kind of communications prone to more attack.
3. Most of the present VANET systems do not provide good enough security extension to prevent the privacy leakage, to prevent miss information being spread and to prevent vehicles from spreading false or intruding messages. Therefore, there is a need of new architecture which provides better security to existing VANET architecture by introducing vehicle to infrastructure architecture alongside vehicle to vehicle collaborating model.

5. Methodology

- MAP MODULING: The role is to take open street map component from 'openstreetmaps.org' and render it.
- TRAFFIC LIGHTS: Add the traffic lights at the junctions with three controls i.e., red, yellow, green.
- VEHICLES: The vehicles will be Wi-Fi enabled. That can read both location data and as well as event data and event data will have higher priority.
- PRIVACY PROTECTION:
  - → To prevent the leakage of vehicle's identity.
  - → To detect spam event data.
- RSU: It acts like Wi-Fi repeater and communication range is increased.
- INTRUSION DETECTION SYSTEM: Comparing all the messages received from all the nodes.
- STATISTICS: shows the latency and packet delivery ratio.
- MIX ZONES: It symbolizes the public places where the Wi-Fi is password free and can cause the data leakage.
- ROUTING MODEL: The algorithms used here are;
  - → ACO (Ants Colonies Optimization)
  - → AES (Advanced encryption standard)

6. Graphs

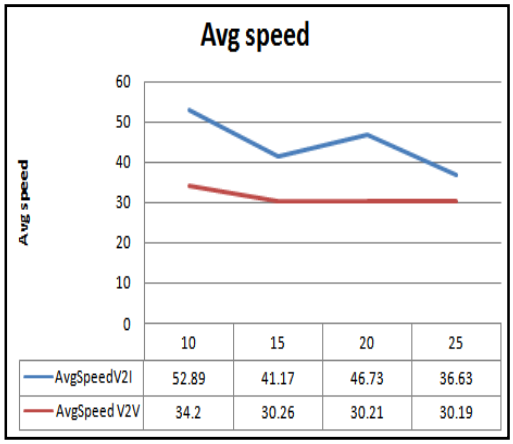

Figure 1 : The graph shows average speed of v2v and v2I

As the number of vehicle increases the average speed will decrease in any network, say if we have 100 vehicles average speed is much more less the 10 vehicles but because whole VANET system it manages the traffic lights in a such way that it routes the vehicles which road to go such that almost every vehicles gets the better road. Therefore, we can always have better proposed system when there is RSU, RSU routes better way. So we have better average speed.

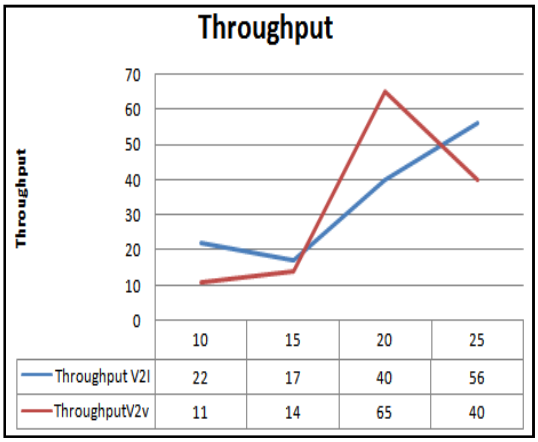

Figure 2 : The graph shows throughput

It defined as number of bits transmitted per second. In V2V communication ideally too many vehicles exchange he number of packets because they are routed through vehicles only. More number of bits can be transmitted at given instance of time. Throughput of V2I is high however number of vehicles data has to wait in queue it can transmit before it transmits to another because if we have 10 vehicles and each vehicle want to communicate with other the amount of links is required to huge when the link is huge under that condition throughput decreases. For the present system number of vehicle increases throughput decreases drastically. In the proposed system the number of vehicle increases the RSU transmits the more vehicles the RSU always transmits the broadcast way. Therefore, throughput increases.

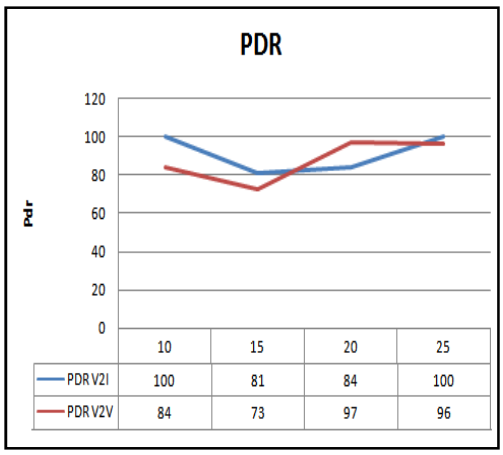

Figure 3 : The graph shows packet delivery ratio.

The PDR for large number of vehicle is nearer to 100%. The PDR ideal value should be 100%. The PDR is defined as the number of delivered packet *100/number of transmitted packet. When the number of vehicles start increasing the interference starts getting increases because of that number of few losses now the losses will have the wide reasons, neither is close to vehicle nor close to RSU the packet is going to be dropped as the number of vehicles become moderate the PDR start getting increase. Because there is complete connectivity in the network.

If we have moderate number of vehicles under that situation there is no packet drop but in the case of V2I communication the vehicle will be always try to find the RSU. Now because there are too many number of vehicles trying to search for RSU the packet delivery ratio will drop because the RSU connection is shared by many number of vehicles for moderate number of vehicle the PDR for pure V2I communication is better than the V2V communication.

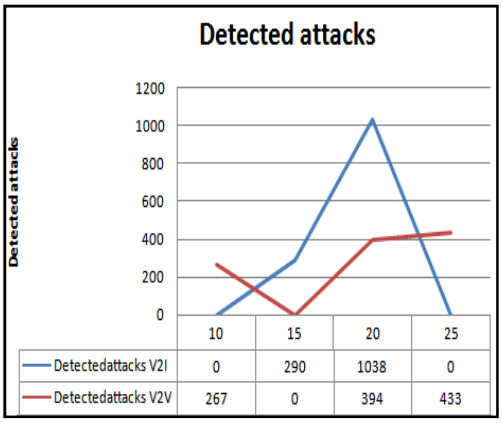

Figure 4 : The graph shows detected attacks

For moderate number of nodes the attack is going to be detected properly. Whenever the number of nodes increases the detected attack decreases linearly

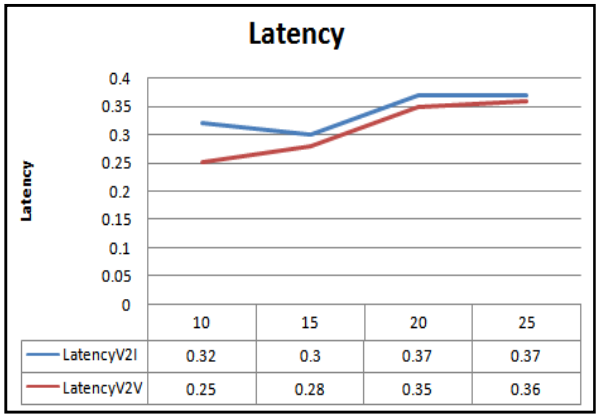

Figure 5 : The graph shows the latency

Latency ideally increases as the number of vehicles increases but because of proper data management of the VANET the latency is not increasing clearly.

From this we can prove that VANET can not only help to traffic signals by controlling the congestion and by controlling the light the system always provides the good throughput the data is always is real time. There is not much latency the data can be received within 60milisec. So we can basically transmit about 10 packets per second. We can transmit 10-15 packets per sec so it is good amount of data transmission. So the event can be tracked real time. Because the event can be tracked real time from scenario e can get the vehicles will always from the before where ever damaged road is there. Therefore, it makes traffic smoother. We can also find out due to proper management of the vehicular ad hoc network the vehicle speed will never fall down because of the increase in vehicle the packets can be transmitted with good enough accuracy so there is no accuracy problem here at the same time we make a cluster of moderate number of vehicles we can always detected attacker within a small group of vehicles.

7. Applications

Assisting the vehicle to go to their destination through an optimum path which is not a hazardous road and no traffic congestion. The work can be used to efficiently control the city traffic lights such that in every junction the vehicle flow is consistent and can move with constant enough speed across any junction and throughout the city. The work can be used to mitigate information data within local navigation

system such as the information about the hospitals, school zones, petrol bunks, etc. The system can be used to mitigate the information about critical city traffic scenarios such as road accidents, severe road congestion due various city conditions. The work can further be used for navigational information such that the vehicles could locate the ideal path to specific destination, this is better than the conventional navigation service because the VANET also incorporates the number of vehicles already there on the path so that the vehicle can decide based on the congestion level to take the specific roads or not. The work can also be used to ensure the secure communication among the large number of communicating devices by incorporating the security framework monitored by RSUs. This system can also be used to avoid the misinformation or privacy leakage in mix zones such as the open Wi-Fi zones that are available nearby airports and shopping malls, etc.

8. Conclusion

Vehicular ad-hoc network has been a recent a phenomenon for managing the city traffic in a distributed way. However, it is often found that vehicle-to-vehicle communication oriented traffic management results in huge amount of communication overhead and packet drops due to inefficient routing in VANET architecture, this situation is further worsening due to security threats because of open Wi-Fi and mix-zones present in the VANET architecture. Therefore, in this work we have proposed a noble architecture through V2I communication system by means of which the security is provided by the RSUs and these RSUs collaborates with V2V communication system to offer better packet delivery ratio and as well quick delivery of critical data messages. The system can be further improved by incorporating more stagnant algorithm for security such as rule based security techniques and machine learning based techniques whereby new attacks can be easily detected.

9. References

i. Wang, D.Zeng, and L.Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update", IEEE Pervasive Computing, Vol. 5, No. 4, pp. 68 – 69, 2006.
ii. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC Packet Communication System for ITS Services," in Proceedings of the IEEE VTC '99, Sept. 1999, pp. 2223 – 2227.
iii. Leontiadis, P. Costa, and C. Mascolo, "Extending Access Point Connectivity through Opportunistic Routing in Vehicular Networks," in Proceedings of the IEEE INFOCOM '10, Mar. 2010.
iv. W. Chim, S.M. Yiu and Lucas C.K, Hui Victor O.K. Li, "VSPN: VANET based Secure and Privacy-preserving Navigation"
v. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An Efficient Identity based Batch Verification Scheme for Vehicular Sensor Networks," in Proceedings of the IEEE INFOCOM '08, Apr. 2008, pp. 816 – 824.
vi. Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran "AMOEBA: Robust Location Privacy Scheme for VANET"
vii. Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, Kaoru Sezaki. "CARAVAN: Providing Location Privacy for VANET"