A Density based Deceptive data Detection in VANET

A.Sravya, K.Dinesh, S.Shiva Prasad

ABSTRACT--- The wireless network is the backbone of the VANET has shown more deceptive data send by malicious node. Those deceptive data may lead to unreliable wireless communication and also inaccurate sensing at the data. Therefore, it is important for detecting the deceptive data and improve the quality of the data in the VANET. So, in order to find those deceptive data in the VANET, there are different types in security aspects and reputation-based approaches, it is not sufficient for managing the quality of data in highly distributed and dynamic environment like VANET hence new algorithm had been proposed for verifying the deceptive data in VANET. The aim of the proposed algorithm is to find the deceptive data about the accident report generated in the VANET. So, as per the VANET mechanism if the accident happened, the accident report is sent from the accident vehicle or node through their sensor to the nearby vehicle and RSU [Road side unit]. The accident report is passed to nearby vehicle through the inter-vehicle communication or vehicle-infrastructure communication. Then the communication is divided into two types such as vehicle to vehicle communication (V2V) and vehicle-infrastructure communication (V2I). The density based deceptive data detection on VANET can be divided into two categories such as dense and spare parts. The dense parts use the clustering technique for finding the deceptive data over the communication whereas the sparse parts utilize the new technique by categories the nodes into two types such as private and public vehicle.

Keywords: clustering, deceptive data algorithm, dense and sparse data, VANET.

I. INTRODUCTION

The most prominent usage of the wireless network in the real world application has provided some disadvantage. Especially in the field of the Vehicular Ad-Hoc Network (VANET) the quality of the data collected at the real time scenario is more important for sensing the traffic at particular time. The nodes or vehicle in the VANET performs the intervehicle and vehicle to infrastructure communication. The Road Side Unit (RSU) is used as the main infrastructure for the VANET in order to perform the vehicle to infrastructure communication. The aim of the proposed algorithm is to find the deceptive data about the accident report generated in the VANET. So, as per the VANET mechanism if the accident happened, the accident report is send from the accident vehicle or node through their sensor to the nearby vehicle and RSU. The accident report is passed to nearby vehicle through the inter-vehicle communication or vehicle-infrastructure communication. Every vehicle has its own licence number or vehicle id is fixed with the on-board unit which cannot be altered at any situation. Thus the purpose of the vehicle id is used to uniquely identify the vehicle in the vehicular ad-hoc network.

Once an accident taken place, then the accident report is send from the accident vehicle to its nearby vehicle and Road side unit. The aim of the on-board unit is to establish the communication with the RSU and other vehicle for sending the safety message over the VANET. The practical scenario of fixing the sensor may be fixed anywhere in the vehicle but it should not be damaged in accident. The researchers released that the sensor has been deployed in the manner which can send the signal even the vehicle is completely damaged. The role of the on-board unit has to follow the specific rule during the communication process and also process it in appropriate time. This capability of on-board unit depends upon computation ability, storage size, communication ability and trusted level. However, each sensor plays the corresponding role for which it is assigned in the communication process.

Vehicular Ad-Hoc Network (VANET) is one of the important real world problem which has to send trusted information over the network. So in the proposed system, the vehicles are divided into two categories based on their roles such as Regular vehicle and Public vehicle. Initially, the public vehicle are considered as the trustier vehicle in the communication problem rather than the regular vehicle. Because the regular vehicle are private owned vehicle that can be convinced by malicious vehicle. So we are assigning the higher priority to public vehicle in the proposed system.

In modern day research, VANET is emerging technique with different useful application for the safety of road transport. It is based on the decentralized network structure for communication of VANET. The various types of communication involved in the VANET are cellular network, vehicle to roadside infrastructure and ad hoc vehicle communication. The important process of vehicle in the VANET is to frequently have communication with the other vehicle in the network. Similarly, if the accident happen then the corresponding vehicle has to send accident report to nearby Road Side Unit (RSU). The accident report should be in the format <ID, Role, Message> where ID denotes unique identification number, Role denotes role of the vehicle which is regular or public vehicle and Message denotes communication report of the vehicle to others (i.e.) the message details denotes the accident report. There might a constant value for the public and private vehicle report in

Revised Manuscript Received on February 11 , 2019.

A.Sravya Department of CSE, Vignan Foundation for Science and Technology, Guntur, A.P, India. (E-mail: dineshhumar@gmail.com)

K.Dinesh, Department of CSE, Vignan Foundation for Science and Technology, Guntur, A.P, India.

S.Shiva Prasad, Department of CSE, Vignan Foundation for Science and Technology, Guntur, A.P, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

the network. The constant value holds higher priority for the public vehicles and lower value for the private vehicles

II. LITERATURE SURVEY

The advancement of vehicles and mobile Ad Hoc network technology, the Vehicle Ad hoc Network (VANET) has turned into a rising field of study. This is a difficult problem for searching and managing an effective way to transport some information. A new routing protocol for VANET CBR (Cluster Based Routing) is used [1]. There are Cluster-based directional routing protocol (CBDRP) for highway situation, in which the header of a cluster selects another header according to the moving direction of vehicle to forward packets [2]. The address scheme is a challenge in networks like VANET. Dynamic Auto-Addressing Plan for VANET Incoming Vehicles attempts to achieve the need for auto IP address configuration with the help of clustering process by allocating specific IP addresses to the time zone dynamic addressing scheme, VANET is attractive for time-critical applications for VANET networks and mobility and fixed infrastructure. Concerning to node obstacles via transport infrastructure, VANET anticipates the survival of fixed factors in infrastructure so referred to as RSU (Road Side Unit)(3) a navigation scheme that makes use of the online road in sequence gathered by a vehicular ad hoc network (VANET) to manual the drivers to desired destinations in a real-time and distributed manner. The proposed scheme has the gain of the usage of real time road situations to compute a better path and on the same time, the information supply can be properly authenticated [4]. Routing based totally on clustering is appropriate for vehicular networks as vehicles may appearance clusters on road. The advantages of clustering can be summarize as follows [5]: (i) clustering can facilitate the reuse of resources after which can enhance the ability of VANET, (ii) clustering can reduce the amount of information that is used to store the network state, (iii) the quantity of routing information propagated in the network can be reduced in cluster- based routing, (iv) a cluster-head (CH) can collect the status of its members and build an overview of its cluster circumstance and (v) distant vehicles outside a cluster usually do not need to recognize the details of particular activities taking place inside the cluster. Inside the clustering algorithm every cluster includes of cluster head (CH) and some individuals [6] In VANET, three communication modes, i.e., vehicle to vehicle (V2V) communication, vehicle to infrastructure (V2I) communication and hybrid vehicle (HV) communication are predictable to be supported to provide users with safety related applications such as accident warning, road congestion control, intersection reminder, etc., and user information related applications such as internet connectivity and peer-to-peer applications, etc[6] The utility function of vehicles is formulated which collectively considers present state of vehicles characterized by the vehicle degree, relative velocity and position between adjacent vehicles, and long-term transmission performance of vehicles, defined as credit history characteristic, that’s characterized through the average available bandwidth, queue length and the duration for being a cluster head (CH) in a past period. The manner of cluster forming is presented, and the vehicles with large utility function are selected as CHs successively [11].

III. PROPOSED SYSTEM

The proposed algorithm aimed for enhancing the performance and safety of Intelligent Transportation System (ITS). In the Vehicular Ad-hoc network (VANET) each node or vehicle broadcast the status message to all the nearby vehicle and also to the roadside Units (SRU). The communication process is mainly depending upon the flooding mechanism (i.e.) each vehicle in the network broadcast their status message in the network. There are two types of communication is applicable in the VANET such as vehicle to vehicle communication and vehicle to infrastructure communication. The major problem in the VANET is large number of messages flooding the network. So, the rate of deceptive in the network also increases. The main goal proposed system is to find the deceptive data in the network based on the density of the network. However, the density plays an important role for finding the deceptive data over the network. So, the proposed density based deceptive data detection system is majorly divided into two type (i.e.) dense and sparse parts. It is based on the density of vehicle at various position of VANET. The concentration of vehicle is high at the dense parts whereas the density is low at sparse parts which can be divided on the basics of cluster formation approach. The stability of cluster formation holds good at dense parts and it has been for finding the deceptive data but in the spare parts the vehicle are majorly distributed as public and private vehicles. In practice, the public vehicle are most trustable vehicle while the private vehicle are not trustable because of its personal usage. Each vehicles in the Vehicular ad-hoc networks are communicated using broadcast hello message. Besides, the hello message consists of the information such as vehicle id (id_v), weight (wt_v), clusterhead id (id_ch) and the current time (Cur_Time). And also the vehicle which receives the hello message stores the vehicle id into the neighbour list (neigh_v). Similarly, the accident reports are broadcasted to all the vehicle, clusterhead and RSU of the network. The accident report (Ar) are broadcasted immediately across the network with the detail like position of the vehicle (v_pos). Then each node involved in the accident send the accident report to the RSU and broadcast the status to other vehicle in the network. Further the actual position of the accident place are adopted from the accident report (Ar) which can be further utilized to find the dense and sparse parts of the network.

The main role of cluster formation is to allow the cluster member for additional exploration of the new node to the clusterhead. In this approach, the new node belongs to the unidentified vehicle among the cluster member should wait for 4 beacon time period for receiving the hello message from other nodes. For example, if the node received the hello message from the vehicle and also checked whether it also the member of any cluster. In case 1, the node is the member of the cluster member then the node send the join message to the cluster head. Next if the node is not belong to any cluster member then it should whether the weight of is greater than the node (i.e.) if the condition is true then the vehicle chooses same the cluster head as . Otherwise, the node declare itself as clusterhead and the node send the join message to it.

The join procedure is responsible for adding the nodes as the cluster member of the cluster. Then the every vehicle or node joining the cluster is assigned to the cluster head id (and load the information about the member such as id, weight, position, velocity, time and dominance value. On the other hand, if the vehicle is already in the history of cluster member then values are updated. The dominance value (C_Dom_VAL) of the cluster member is referred as the average weight and velocity, which have been used to rank.

Further the freshness of all the cluster member are calculated using the procedure Freshness (). Every nodes in the cluster has to establish the proper communication with the cluster head and other members. In some cases, if the vehicle is not sending the hello message or moved from one the cluster members cluster to another has been removed from the cluster periodically. So, the freshness of the vehicle is calculated at regular intervals of time. But if the vehicle is not shown the visibility for more than 4 beacon time period then it has been removed from the cluster members (i.e.) if the last seen time (LST) of cluster is less than freshness estimated time then the vehicle id is removed from the cluster member. Similarly, the freshness has been estimated to cluster head but the freshness time is reduced when compared with the cluster member (i.e.) if the cluster head is not responding for the cluster member request for more than 3 beacon time period then the cluster head (id_ch) is reinitialized to NULL. In addition to this process, the cluster head change process has been initialized to reassign the cluster head to the cluster where the vehicle having the maximum dominance value has been selected as the head and also change the cluster head id of all the cluster members.

A. Accident Detection

The vehicular ad-hoc network (VANET) consists of the deceptive data which has been flooded within the network reduces the quality of information. Sometimes the intruders in the network also want to send the malicious report over the network in order to divert the concentration of central servers and RSU. So the proposed is aimed to find the deceptive data over the VANET by using the density based deceptive data technique. Once if the accident happens than the corresponding vehicles involved in the accident send the accident report (Ar) to the nearby Road Side Unit (RSU) and other vehicles. Then the RSU detect the actual location of the accident place using the accident report and also the find whether it belongs to sparse or dense part of the network. Further, the distance between the RSU to accident place (D1) and accident place next RSU(D2) has been calculated.

B. Sparse parts

In this technique, the actual flow of comparatively lesser than the dense part so the average flow of the vehicle has been estimated between two Road Side Unit R1 and R2. Then each vehicle between two RSU has been divided according the categories such as regular vehicle and public vehicle. Therefore the actual number of regular and public vehicle within the two RSU has been evaluated. The vehicle flow ( ) is calculated between the two RSU by counting the flow of regular and public vehicle. Hence, the vehicle flow is lesser than the ¾ average flow of vehicle (Avg_ Cv) then the accident is occurred otherwise it not.

C. Dense parts

The dense parts consists of high node density within the network so the clustering technique has been utilized for finding the deceptive data about the accident report. Then average flow of cluster members between two RSU has been estimated. If the flow of vehicle is between the two RSU then the number of vehicle belong to the cluster member and cluster head has been estimated. Thus the flow of vehicle is lesser than ¾ average flow of vehicle (Avg_Cv) then the accident is happen else it is not. Hence, the proposed system uses the dense and sparse technique for finding the deceptive data over the VANET.

IV. EXPERIMENTATION

In order to implement our proposed system we uses VANET simulator called a traffic simulator. We design our simulator by extending a traffic simulator that simulates the movements of the vehicles, such as acceleration, deceleration, speed and lane changing. In addition, we simulate the scenario of accidents, as well as malicious vehicles .We ran the implementation on an Intel Pentium (R) D 2.5Ghz machine with 4.0 GB RAM desktop PC with 100 MB/s Ethernet card, Window7 and IDE Eclipse Kepler version 4.3 to produce GUI for our proposed system. As our proposed system is based on three approach namely density, Redundancy within the range and redundancy outside the range we use matlab to implement these proposed approach and compared the result with the existing approach.

In our experiments, the communication between the vehicles follows vehicle to infrastructure communication. The RSU will be placed in the particular distance along the side of the road. In our traffic simulation we designed for each vehicle the speed limitation is 120 km/h. The road segment consists of a U-shape road with the length of 6575 m. When an accident appears, the road will be blocked for several minutes. The malicious vehicles will periodically broadcast a fake accident report.

In MATLAB, we calculated the number of vehicle flow and the redundant message send from each vehicle and density of vehicles within the range and we also calculated the velocity which is the existing system and compared our proposed system with the existing system to show the effectiveness and efficiency of our proposed approach.

A. Traffic micro simulation

In our simulation we use traffic micro simulation called traffic simulator. Traffic micro simulation models simulate the behavior of individual vehicles within a predefined road network and are used to predict the likely impact of changes in traffic patterns resulting from changes to traffic flow or from changes to the physical environment. Micro simulation also reflects even relatively small changes in the physical environment such as the narrowing of lanes or the relocation of junction stop lines.

B. Performance Assessment Criteria

The performance assessment criteria is given to detect the false accident reports inserted by malicious vehicles and confirms the true accident reports generated by the vehicles involved in the accident. This property is evaluated by both communication parameters and deceptive data parameters.

Communication parameters include throughput, Packet reception ratio and deceptive data detection parameters include recall. Let us discuss in detail about both communication parameters and deceptive data detection parameters. Here in the table below Table 1. we showed the sample results of our density technique and comparison is made with the original report and existing approach.

V. RESULTS & DISSCUSSIONS

Original Report	**Velocity**	**DENSITY**		
		Average flow	***Actual Flow***	***Report***
FALSE ACCIDENT	FALSE ACCIDENT	240	385	FALSE ACCIDENT
TRUE ACCIDENT	TRUE ACCIDENT	540	267	TRUE ACCIDENT
FALSE ACCIDENT	TRUE ACCIDENT	830	936	FALSE ACCIDENT
TRUE ACCIDENT	TRUE ACCIDENT	740	455	TRUE ACCIDENT
FALSE ACCIDENT	FALSE ACCIDENT	980	1202	FALSE ACCIDENT
FALSE ACCIDENT	FALSE ACCIDENT	850	357	FALSE ACCIDENT
TRUE ACCIDENT	TRUE ACCIDENT	440	249	TRUE ACCIDENT
FALSE ACCIDENT	TRUE ACCIDENT	270	262	TRUE ACCIDENT
TRUE ACCIDENT	TRUE ACCIDENT	340	199	TRUE ACCIDENT
TRUE ACCIDENT	TRUE ACCIDENT	410	287	TRUE ACCIDENT
TRUE ACCIDENT	TRUE ACCIDENT	940	712	TRUE ACCIDENT
FALSE ACCIDENT	FALSE ACCIDENT	780	977	FALSE ACCIDENT

B. Data Detection parameters

In our system when an accident happens our aim is to detect whether the accident is really happen or not. Malicious vehicles in our system will broadcast false report to divert the concentration of central board. Our deceptive data detection parameter is used to find the true report from false report, deceptive data detection parameters includes recall and precision.

Recall:

Recall is defined by the proportion of relevant results that have been retrieved. The general notation for recall is given as

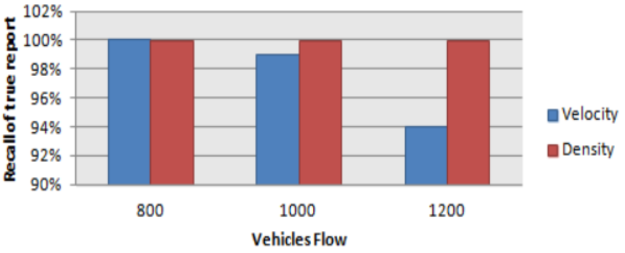
$$Recall = R = \frac{relevant\ retrieved\ results}{relevant\ results\ in\ database}$$

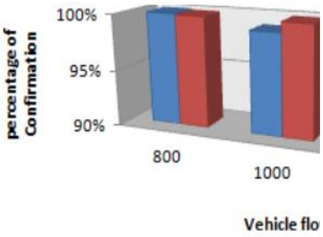
where SPQur is the number of successfully retrieved services for the query Qur and FAQur is the number of services that fail to be retrieved by the matchmaker for the query Qur.

Recall can be explained with an example recall is defined as the ratio between relevant retrieved to the total relevant results in the database. Let us consider the relevant result be true accident. Here the total messages received in our system with true and false accident report is 2044. True accident report retrieved is 1134 and total true accident report received in the database is 1134 So the relevant retrieved message is 1134 and total relevant results in the database is 1134. So the recall is 1134/1134. From here we can come to a conclusion about the proportion of relevant results that have been retrieved in our system.

The Recall value lies between 0 and 1 and are normally expresses as percentages. To be specific in this application, the recall of false accident reports is defined as the fraction of the false accident reports that is detected by our proposed approaches while the recall of true accident reports is defined as the fraction of true accident reports confirmed by our proposed approaches.

The graph shows the recall of our proposed system and compared our result with the velocity based technique. When the number of vehicles increases our technique shows greater results than the existing technique.





Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VI. CONCLUSION

The proposed density based clustering approach for VANET is based on the vehicle to infrastructure communication. The vehicle can send safety message over the network for the efficient transportation system. . As the assumption of VANET, the vehicle can able to send message or report at any circumstances so the vehicle which is damaged in accident send the report to the nearby Road Side Unit (RSU). The RSU has been utilized for discovering whether the accident takes place in sparse or dense parts. Then by depending upon the sparse or dense parts the appropriate technique has been used for finding the deceptive data. In Future, this techniques can further be enhanced using internet of things.

VII. ACKNOWLEDGEMENT

This is a text of acknowledgements. Do not forget people who have assisted you on your work. Do not exaggerate with thanks. If your work has been paid by a Grant, mention the Grant name and number here.

REFERENCES

1. Nafi, N. S., & Khan, J. Y. (2012). A VANET based intelligent road traffic signalling system. Australasian Telecommunication Networks and Applications Conference, ATNAC 2012. http://doi.org/10.1109/ATNAC.2012.6398066
2. Ucar, S., Ergen, S. C., & Ozkasap, O. (2016). Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination. IEEE Transactions on Vehicular Technology, 65(4), 2621-2636.
3. AlMheiri, S. M., & AlQamzi, H. S. (2015, February). MANETs and VANETs clustering algorithms: A survey. In GCC Conference and Exhibition (GCCCE), 2015 IEEE 8th (pp. 1-6). IEEE.http://doi.org/10.1109/IEEEGCC.2015.7060048
4. Chai, R., Ge, X., Hu, X., & Yang, B. (2014, August). Work in progress paper: Utility based clustering algorithm for VANET. In Communications and Networking in China (CHINACOM), 2014 9th International Conference on (pp. 187-190). IEEE.
5. Conference on Communications and Networking in China, CHINACOM 2014, 187 190. http://doi.org/10.1109/CHINACOM.2014.7054283
6. Wang, C., Li, X., Li, F., & Lu, H. (2014, September). A mobility clustering-based roadside units deployment for VANET. In Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific (pp. 1-6). IEEE.
7. Sood, M., & Kanwar, S. (2014). Clustering in MANET and VANET: A survey. 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications, CSCITA 2014, 375–380. http://doi.org/10.1109/CSCITA.2014.6839290
8. Chai, R., Yang, B., Li, L., Sun, X., Chen, Q., Rong Chai, … Qianbin Chen. (2013). Clustering-based data transmission algorithms for VANET. 2013 International Conference on Wireless Communications and Signal Processing, (61102063), 1–6.
9. Yang, Y., Li, H., & Huang, Q. (2013). Mobility management in VANET. Proceedings - 2013 Wireless and Optical Communications Conference, WOCC 2013, 298–303. http://doi.org/10.1109/WOCC.2013.6676326
10. Sahoo, R. R., Panda, R., Behera, D. K., & Naskar, M. K. (2012). A trust based clustering with Ant Colony Routing in VANET. 2012 3rd International Conference on Computing, Communication and Networking Technologies, ICCCNT 2012, (July). http://doi.org/10.1109/ICCCNT.2012.6395939
11. Chim, T. W., Yiu, S. M., Hui, L. C. K., & O.k. Li, V. (2014). VSPN: VANET-based secure and privacy-preserving navigation. IEEE Transactions on Computers, 63(2), 510–524. http://doi.org/10.1109/TC.2012.188
12. Janech, J., Lieskovsky, A., & Krsak, E. (2012). Comparation of strategies for data replication in VANET environment. Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012, 575–580. http://doi.org/10.1109/WAINA.2012.179
13. Bugti, S. A., Chunhe, X., Wie, L., & Hussain, E. (2011). Cluster based addressing scheme in VANET (CANVET stateful addressing approach). 2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011, 450–454. http://doi.org/10.1109/ICCSN.2011.6013754
14. Song, T., Xia, W., Song, T., & Shen, L. (2010). A cluster-based directional routing protocol in VANET. International Conference on Communication Technology Proceedings, ICCT, (2008), 1172–1175. http://doi.org/10.1109/ICCT.2010.5689132
15. Luo, Y. L. Y., Zhang, W. Z. W., & Hu, Y. H. Y. (2010). A New Cluster Based Routing Protocol for VANET. Networks Security Wireless Communications
16. Sha, K., Wang, S., & Shi, W. (2010). RD4: Role-differentiated cooperative deceptive data detection and filtering in VANETs. IEEE Transactions on Vehicular Technology, 59(3), 1183–1190. https://doi.org/10.1109/TVT.2010.2040400