ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

False Node Identification in VANETs for Securing Warning Messages

Rajimol R, Vinodh P Vijayan

M. Tech Student, Dept. of CSE, Mahatma Gandhi University, Mangalam College of Engineering, Kottayam, India.

Associate Professor, Dept. of CSE , Mahatma Gandhi University, Mangalam College of Engineering, Kottayam, India.

ABSTRACT: The greatest challenge of vehicular adhoc network is to identify the false node in the network. These false nodes can create many dangerous situations to the vehicles. The solution for this is the F measure based VANET. F measure group the se of nodes into clusters and assign a weight to each node based on the conflict in the network. The highest conflict causing node set will get highest weight value and those node set will considered as false nodes in the network. This allows the network to detect false nodes more accurately with maximum precision and minimum recall. System uses a half encryption technique to reduce the time complexities in the network. This helps to improve the accuracy and efficiency of the network.

KEYWORDS: Vehicular adhoc network, F measure, half encryption, recall, precision, clustering

I. INTRODUCTION

Vehicular adhoc network (VANET) is a type of wireless network and it requires minimum infrastructure for setting up a network. VANETs based on F measure technique helps to detect the false nodes more accurately from the network. System includes the calculation of precision and recall in order to reduce the errors in the system. It also uses half encryption to reduce the time complexities.

System uses two types of messages for sending the position and keys between the nodes in the network. With the information obtained by those messages, each node tries to identify whether its neighbours are false or not. Firstly it uses a direct method for identifying the false nodes based on the communication range of each node in the network. Then it uses a n indirect method, which compares two of the neighbours with itself. If any conflict occurs, then it marks that node as false. System also uses a mismatch count based technique. In this, mismatch count of each node is calculated and the node having highest mismatch count is set as false node.

In F measure based technique, system groups the nodes into different clusters and each cluster is analyzed repeatedly. Whenever it identifies a conflict node, then assign a weight to it. The weight of each node is incremented when the conflict arises due to that node increases. Thus the system forms different clusters with high weighted node set. Thus the node set with highest weight is considered as the false nodes.

II. RELATED WORK

Securing warning message dissemination in VANET using CNPV algorithm helps to identify the node that provides wrong information system [1]. CNPV algorithm works in two rounds. During these rounds, each node transmits their public and private keys, nodes positions, node id etc. By using this information system can identify the node that passes inaccurate data. The main aim of CNPV is to locate the position of the neighbour node and to verify them as true or false.

VANET based ambient ad-dissemination system provides security for the ad-dissemination with pragmatic cost and effect control [2]. System uses distance based gradient algorithm for improving the effect of ad dissemination. It also uses privacy preserving cash- in algorithm to provide cooperation among vehicles in the network.

Cryptographic mechanism used in VANET helps to detect Sybil attack efficiently [3]. Sybil attack introduces false identities to the system. There by it can create an impression that there are many other vehicles in the network. This can create danger situation to the vehicles in the network. Sybil attack detection based on cryptographic mechanism provides some security aspects such as authentication, data integrity, non repudiation and privacy.

Nonline of sight (NLOS) verification in VANET using secure cooperative approach provides security and integrity to the localization service [4]. NLOS is a state created by obstacles in the road between vehicles, which will results in non-sharing of information between the nodes. Cooperative local verification helps to trigger the verification process and avoiding the acceptance of errors.

OppCast in VANET helps to achieve maximum warning message packet reception ratio and fast message propagation with minimum number of transmission [5]. It also uses double phase broadcast strategy for getting fast propagation of messages in one phase and to achieve maximum packet reception ration in another phase. Broadcast acknowledgements are also provided to avoid repeated transmissions.

Graph based metric used in VANET for the detection of insider attacks [6]. System uses a baseline protocol, a geocast protocol and aggregation protocol. This system provides a communication redundancy for multihop protocols. This redundancy is very helpful to obtain the consistency of data. Base line protocol helps to identify the maximum redundancy in the network. Geocast protocol helps to estimate the probability of data forwarding by each node. Aggregation scheme uses the fixed segment of the road in which all changes are visible.

Robust congestion control schemes are used in VANET for fast and reliable dissemination of messages [7]. System consists of three phases- priority assignment phase, congestion detection phase and beacon transmission phase. Beacon messages contain information about the vehicles such as vehicle speed, direction, position etc. Priorities are assigned based on the number of safe messages waiting for transmission.

VESPA approach for VANET helps to share data among vehicles in the network. The goal of VESPA is to transmit data to vehicles that are more urgently required and evaluating the relevance. Aggregation of data in the network helps to identify the dangerous situations in the road [8]. System also provides additional knowledge to the driver. Centralized and decentralized schemes can be used to aggregate the data. In centralized approach, each vehicle send the data to a centralized server. Then the server constructs the aggregate from the available data. But in decentralized approach, each vehicle can construct there on aggregate.

Eviction of misbehaving and faulty nodes in vehicular network helps to improve robustness. System consists of infrastructure based revocation protocol, misbehavior detection system and a LEAVE protocol [9]. LEAVE protocol helps to temporarily evict the neighbour of the misbehaving node.

Vehicular behavioral analysis in VANET helps to detect the trustworthiness of vehicles [10]. Each vehicle can calculate the trustworthiness of its nearest vehicles. For that, outputs of different behavioral modules are combined. Trustworthiness value assigned to each vehicle can be exchanged and based on this vehicles are divided into the categories trustworthy, untrustworthy and neutral.

III. PROPOSED SYSTEM

Vehicular adhoc network (VANET) is a type of wireless network that does not requires any stable infrastructure [1]. Vanet forms a network by connecting different vehicles on the road and used to transmit messages among them as in the form of warnings or data. In order to identify the false node that provide wrong information and to increase the accuracy, system uses F measure based mechanism. It also uses half encryption in order to reduce the time of transmission of messages.

In Vanet, it is very important to detect the position of each node. The most nearest neighbour node can pass correct information to the other node. It is very helpful in road safety and traffic management schemes. But most of the schemes are failed to detect the false node that transmit wrong information to the network. The F measure based proposed mechanism increases the accuracy of detecting such false nodes within small time period.

A. *System Architecture*

System first transmits two types of messages between the nodes in the network. They are HELLO and DISCLOSURE messages as in CNPV [1]. By using these messages each node will get the positions of every other node. System uses different methods to detect the fake nodes. Firstly the system checks whether all the nodes are in the communication range of the network based on the position obtained by each nodes. If not, it will not consider those nodes for the transmission of messages. Then the system checks in an indirect way.

In indirect method, each node checks whether the nodes that passes messages to them are in correct position or not. If it is in same position, then node announces it as true node. Otherwise it announces them as false. But it is not an accurate way for detecting the false nodes. So system uses another method based on the mismatch count.

In mismatch count based method, each node that is identified as false will get a mismatch count. Those nodes that got highest mismatch count will consider as the false node. This method increases accuracy when compared with other two methods. But all these method take large time instance for the execution. So the system uses a new method based on F measure. System also uses half encryption technique to reduce the time taken for execution.

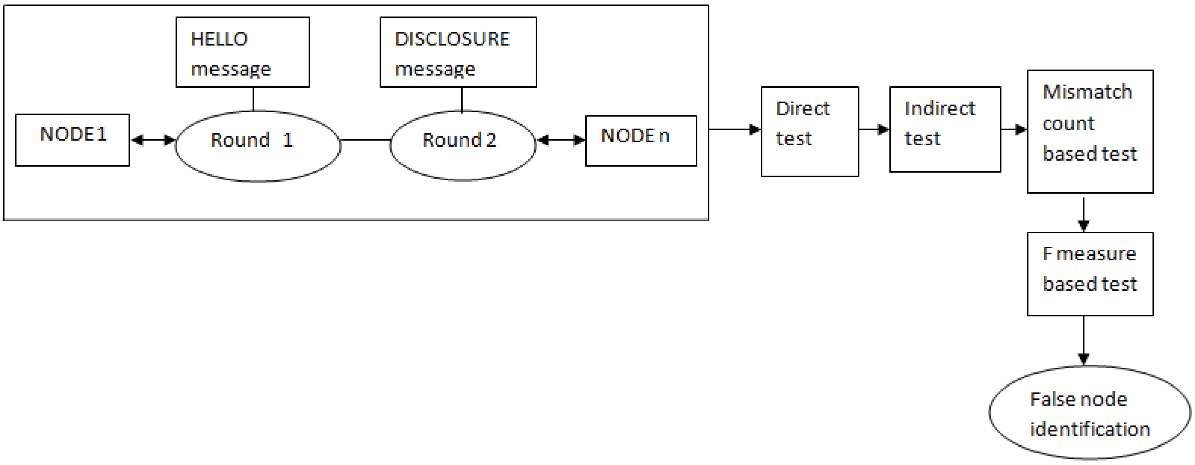

Fig.1. Architecture of F measure based VANET

B. *F measure*

F measure is the mean of precision and recall. Precision indicates the number of nodes that is correctly classified from a set of assumed nodes that is correctly classified. But recall indicates the number of nodes that is wrongly classified from the set of assumed nodes that is correctly classified. It reduces the percentage of false positives. So by reducing the percentage of recall and by increasing the percentage of precision, system can provide more accurate results. So that system can detect most of the fake nodes in the network.

In F measure based technique, it forms each node with its nearest nodes as a small graph with connecting paths. Then it checks whether there is any conflicts or any failure of path is in that graph. If so system selects the node that causes conflicts to the network as a separate group. Systems also rank that node by providing a weight as 1. Then it again checks whether the same node cause any problem to other set of nodes. If so, its rank becomes incremented. On continuing this, the system will get a set of nodes that causes conflicts to the network with a specific weight or rank.

System again performs another clustering on the selected set of conflict causing nodes. It again separates the highest weighted node to another set. Then assign new rank as 1. Again checks the separated nodes as a graph to identify the conflict. If newly separated node again makes any conflict, then the system will increment the node count as 2. By this, system will again get most filtered set that contains most of the fake nodes.

After performing this, system will take the average of the cluster or set. Average will be taking as 4 times the average value calculated, so that all nodes will be in the range. Then based on the average value, it again performs clustering the nodes. First cluster will contains nodes whose value below average and second cluster will contain nodes whose value above average. The node that belongs to above average cluster will contains the fake nodes. There by system detects most of the fake nodes from the network. This method decreases the percentage of false positives. Thus it produces more accurate result.

C. *Half Encryption*

System uses half encryption as a technique to reduce the time taken for the execution of the system. In normal message transmission in Vanet, it takes more time for the execution because it contains large message size and all these messages needs to be encrypted, so it takes more time instant.

Half encryption is a technique that performs one encryption and double decryption. It performs encryption of public and private keys of each node I the sending side. At the receiving side, these keys are retrieved by performing decryption twice. It also improves the security of the system.

IV. Simulation Results

Experiments are conducted on Intel Core i3 processor with CPU of 2.40GHz. The X and Y positions of each node are used to locate the position of each node. The position information and the public and private keys for each node are used as the messages that sent between the nodes. The false node identification in VANET helps to improve the efficiency of the system in many ways. It helps to improve the network performance by reducing the recall and increasing the precision. This also allows the network to detect the false nodes within small time interval.

A. *Precision*

Precision is a measure helps to identify the amount of data that are accurate from the set of assumed results. Precision helps to improve the accuracy of the system by correctly classifying the false nodes. The x axis of the graph shows the number of suspicious or false nodes and the y axis shows the precision of the system. As the number of suspicious nodes increases, precision also increases. Thus the system provides more accurate result than all other existing systems.

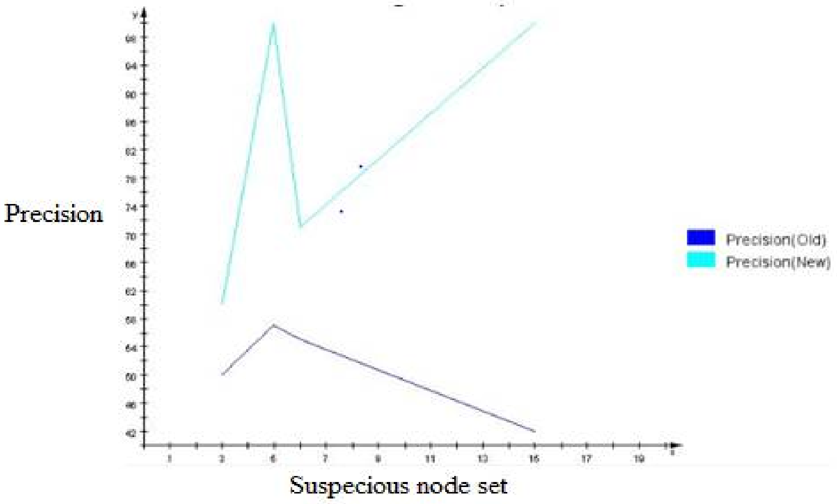

Fig.2. Precision Graph

System uses an F measure technique in order to identify the false nodes in the network. From this obtained F measure, it also helps to detect the percentage of precision. System shows improved precision percentage even if the number of suspicious nodes increases.

First the system performs direct, indirect and mismatch based techniques to identify the false nodes. But all of these techniques show less accurate results. In order to improve the accuracy, F measure based technique is used.

B. *Recall*

Recall is a measure used to identify the amount of data that are not correct from the set of correctly assumed result. It is also called false positive. As the value of recall decreases, the system will produce more accurate results. From the graph it is clear that the recall of the system is always a smaller value for any number of suspicious nodes.

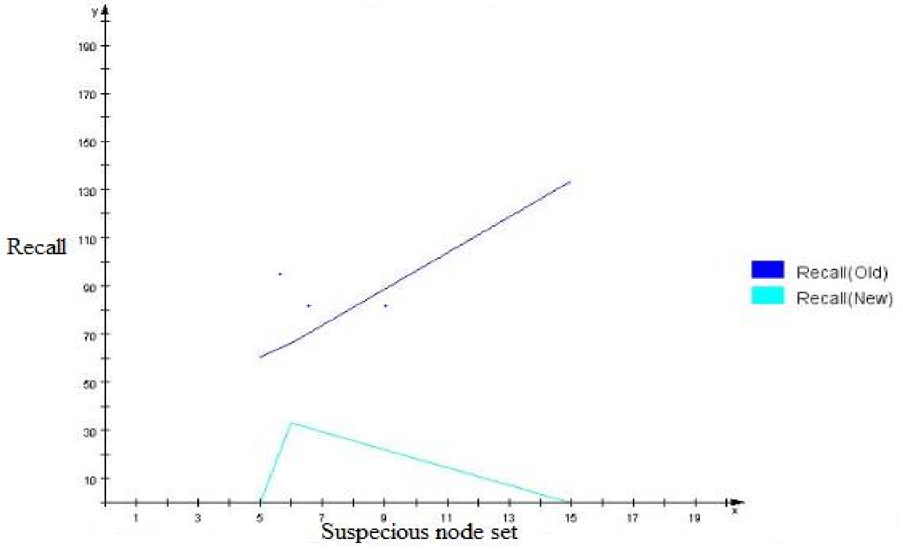

Fig.3. Recall graph

System shows lesser recall rate than other schemes. False positive increases the number of wrongly classified wrong set This system ensures that the it will always produce accurate result. So it reduces the number of false positives in the system.

C. *Encryption Time Evaluation*

Encryption is the mechanism for providing security to the system. It reduces the rate of attacks to the network. The system uses a half encryption technique where one encryption and double decryption is performed. It helps to reduce the time taken for message transmission. In half encryption, amount of data transmitted is lesser than the full encryption. So it also reduces the complexity of message transfer. From the graph it is clear that, for any set of nodes, the time required for half encryption is lesser than old approaches.

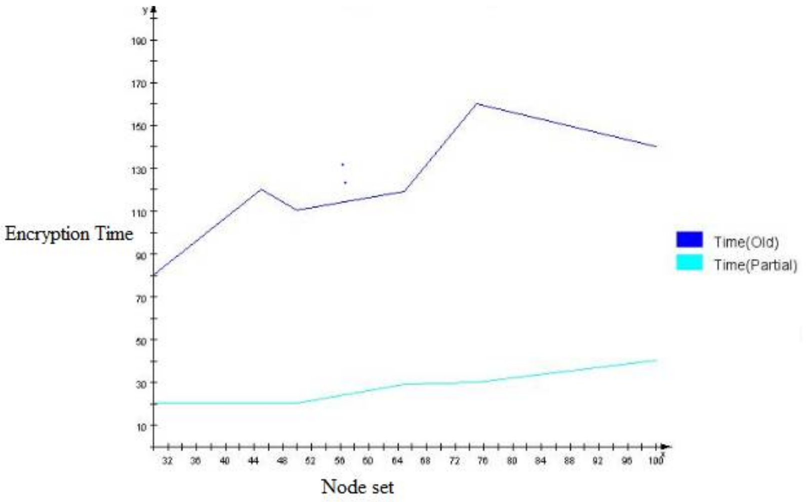

Fig.4. Time Graph

V. Conclusion and Future Work

F measure based vehicular adhoc network helps to detect the false nodes in the system with improved accuracy. This forms different clusters of nodes and based on the weight of nodes, system detect the false nodes. The node set with highest weight will be considered as the false nodes in the network. This detection will take minimum time with the help of half encryption. Half encryption is a technique which performs one encryption and double decryption. Thus it reduces the time and increases the security and performance of the system. F measure based technique helps to reduce the recall and increase the precision for any number of nodes in the network.

In future, it can use different techniques to reduce the overhead of the system by reducing the number of messages transmitted between the nodes in the network.

References

1. Manuel Fogue, Francisco J. Martinez, *Member, IEEE*, Piedad Garrido, *Member, IEEE*, "Securing Warning Message Dissemination in VANETs Using Cooperative Neighbor Position Verification", IEEE transactions on vehicular technology, vol. 64, no. 6, june 2015.
2. Zhengming Li, Congyi Liu, and Chunxiao Chigan," On Secure VANET-Based Ad Dissemination With Pragmatic Cost and Effect Control", IEEE transactions on intelligent transportation systems, vol. 14, no. 1, march 2013.
3. Mina Rahbari and Mohammad Ali Jabreil Jamali," Efficient Detection of Sybil Attack Based on Cryptography in VANET ",International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011
4. Osama Abumansoor, *Member, IEEE*, and Azzedine Boukerche, *Senior Member, IEEE*, "A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET", IEEE transactions on vehicular technology, vol. 61, no. 1, january 2012.
5. Ming Li, Kai Zeng , Wenjing Lou," Opportunistic broadcast of event-driven warning messages in Vehicular Ad Hoc Networks with lossy links", Computer networks, vol 9, no.5, april 23, 2011
6. Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl ," Graph-Based Metrics for Insider Attack Detection inVANET Multihop Data Dissemination Protocols", IEEE transactions on vehicular technology, vol. 62, no. 4, may 2013
7. Soufiene Djahel and Yacine Ghamri-Doudane, "A Robust Congestion Control Scheme for Fast and Reliable Dissemination of Safety Messages in VANETs", IEEE Wireless Communications and Networking Conference,ppt2264-2269, 2012
8. Bruno Defude, Thierry Delot, "Data aggregation in VANETs: the VESPA approach", International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, july 2008
9. M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks" IEEE journal on selected areas in communications, vol. 25, no. 8, october 2007.
10. Robert K. Schmidtx, Tim Leinm¨ullerx, Elmar Schoch, "Vehicle Behavior Analysis to Enhance Security in VANETs", article on telematics and computer networks, sep 2, 2014

BIOGRAPHY

Rajimol R doing M.Tech in Computer science And Engineering at Mangalam College of Engineering, Mahatma Gandhi University. She receives B.Tech degree in 2014 from Mangalam College of Engineering, under Mahatma Gandhi University. Areas of interest are data mining, security and wireless networks.

Vinodh P Vijayan, Associate Professor in Mangalam College of Engineering, under Mahatma Gandhi University. He receives B.Tech from Anna University in 2006 and M.Tech from Anna University in 2008 .

DOI: 10.15680/IJIRCCE.2016.0407133