IJCSEInternational Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

False Node Identification in VANETs for Inmproved Security

Neethu Maria John[1*], Simy Mary Kurian[2], Vinodh P Vijayan[3], Neema George[4]

[1,2,3,4]Department of Computer Science&Engineering, Mangalam College of Engineering, Kerala, India

[*]*Corresponding Author: neethujohn01@mangalam.in, Tel.:+91 9947472025*

Available online at: www.ijcseonline.org

Accepted: 16/Aug/2018, Published: 31/Aug/2018

Abstract— The best test of vehicular adhoc network is to distinguish the false node in the network. These false node can cause numerous perilous circumstances to the vehicles. The answer for this is the F measure based VANET.F measure bunch the se of hubs into groups and appoint a load to every hub in light of the contention in the network.The most noteworthy clash causing node set will get most elevated weight value and those node set will considered as false in the network. This permits the organization to identify bogus hubs all the more precisely with greatest accuracy and least review. Framework utilizes a half encryption strategy to lessen the time intricacies in the network. This assists with moving alongthe exactness and proficiency of the network.

Keywords— F measure, half encryption

I. INTRODUCTION

Vehicular adhoc network (VANET) is a sort of wireless network and it requires least framework for setting up a network. VANETs in light of F measure method assists with identifying the misleading hubs all the more precisely from the network. Framework remembers the estimation of accuracy and review for request to diminish the blunders in the framework. It additionally utilizes half encryption to decrease the time intricacies.

Framework involves two sorts of directives for sending the position and keys between the nodes in the network. With the data acquired by those messages, every node attempts to recognize regardless of whether its neighbors are false or not. Right off the bat it involves an immediate strategy for distinguishing the false nodes in view of the correspondence scope of every node in the network.

Then, at that point, it utilizes a n circuitous strategy, which contrasts two of the neighbors and itself. In the event that any contention happens, it denotes that node as false. Framework likewise utilizes a jumble count based strategy. In this, mismatch count of every node is determined and the node having most mismatch count consider is set as false node.

In F measure based strategy, framework bunches the nodes into various groups and each bunch is investigated over and again. Whenever it distinguishes a conflict node, then relegate a load to it. The weight of every node is augmented when the contention emerges because of that node increments. Accordingly the framework structures various bunches with high weighted node set. Along these lines the node set with most elevated weight is considered as the false nodes

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. 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.

II. RELATED WORK

Getting cautioning message spread in VANET utilizing CNPV algorithm assists with recognizing the hub that gives wrong data framework [1]. CNPV algorithm works in two rounds. During these rounds, every hub communicates their public and private keys, hubs positions, hub id and so forth. By utilizing this data framework can recognize the hub that passes mistaken information. The primary point of CNPV is to find the place of the neighbor hub and to check them as true or false.

VANET based ambient ad-dissemination system provides security for the ad-dissemination with pragmatic cost and effect control[2]. Framework utilizes distance based gradient algorithm for working on the impact of advertisement scattering. It additionally utilizes security saving money in calculation to give participation among vehicles in the organization.

Cryptographic component utilized in VANET assists with distinguishing Sybil attack efficiently [3].Sybil attack efficiently acquaints false characters with the framework. There by it can make a feeling that there are numerous different vehicles in the organization. This can make peril circumstance to the vehicles in the network. Sybil attack location in view of cryptographic system gives some security angles like validation, information honesty, non renouncement and protection.

Nonline of sight (NLOS) confirmation in VANET utilizing secure helpful methodology gives security and uprightness to the confinement administration [4]. NLOS is a state made by obstructions in the street between vehicles, which will brings about non-dividing of data among the hubs. Agreeable neighborhood confirmation assists with setting off the check interaction and keeping away from the acknowledgment of mistakes.

OppCast in VANET assists with accomplishing most extreme admonition message bundle gathering proportion and quick message spread with least number of transmission [5]. It additionally utilizes twofold stage broadcast procedure for getting quick spread of messages in a single stage and to accomplish most extreme bundle gathering apportion in another stage. Broadcast affirmations are likewise given to keep away from rehashed transmissions.

Robust congestion control schemes are utilized in VANET for quick and reliable dissemination of messages[7]. Framework comprises of three stages need task stage, clog identification stage and reference point transmission stage. Beacon messages contain data about the vehicles, for example, vehicle speed, course, position and so forth. Needs are doled out in view of the quantity of safe messages sitting tight for transmission.

Vehicular conduct investigation in VANET assists with recognizing the reliability of vehicles [10]. Every vehicle can ascertain the reliability of its closest vehicles. For that, results of various social modules are joined. Dependability esteem appointed to every vehicle can be traded and in light of this vehicles are partitioned into the classifications reliable, conniving and impartial.

III. PROPOSED SYSTEM

In Vanet, recognizing the place of every node is vital. The most closest neighbor node can pass right data to the next hub. It is extremely useful in street well being and traffic the board plans. Yet, the greater part of the plans are neglected to distinguish the misleading hub that communicate wrong data to the organization. The F measure based proposed instrument expands the exactness of distinguishing such bogus hubs inside modest period.

Framework initially sends two kinds of messages between the nodes in the network. They are HELLO and DISCLOSURE messages as in CNPV [1]. By utilizing these messages every node will get the places of each and every other node. Framework utilizes various techniques to distinguish the fake node. The framework, first and foremost, checks whether every one of the nodes are in the correspondence scope of the network in view of the position got by every nodes. If not, it won't think about those nodes for the transmission of messages. Then the framework checks in a backhanded manner.

In mismatch count based technique, every node that is recognized as false will get a mismatch count. Those nodes that got most mismatch count consider will think about the false node. This technique increments accuracy when contrasted and other two strategies. Be that as it may, every one of these strategy take huge time case for the execution. So the framework utilizes another technique in view of F measure. Framework additionally utilizes half encryption strategy to lessen the time taken for execution.

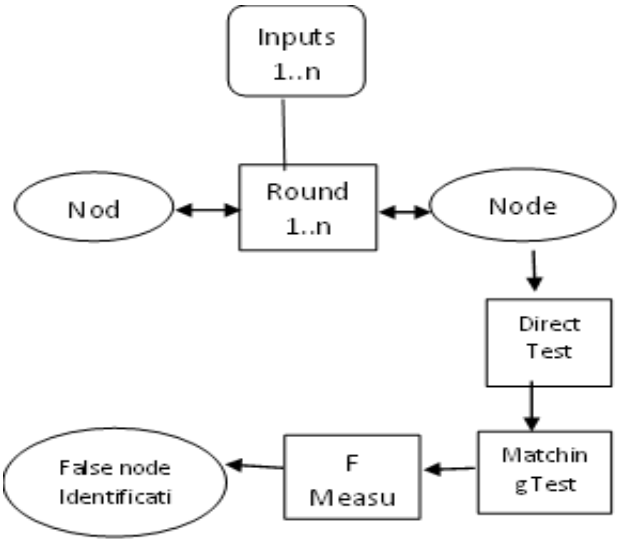

Figure 1:Aarchitecture-F measure

F measure is the mean of accuracy and review. Accuracy demonstrates the quantity of nodes that is accurately grouped from a bunch of accepted nodes that is accurately ordered. Yet, review demonstrates the quantity of nodes that is wrongly grouped from the arrangement of expected nodes that is accurately characterized. It lessens the level of bogus up-sides. So by lessening the level of review and by expanding the level of accuracy, framework can give more precise outcomes. So framework can identify the vast majority of the phony nodes in the network.

In F measure based strategy, it shapes every hub with its closest nodes as a small graph with associating ways.

Then, at that point, it checks whether there is any struggles or any disappointment of way is in that diagram. Assuming this is the case framework chooses the nodes that makes clashes the network as a different group . Frameworks likewise rank that hub by giving a load as 1. Then, at that point, it again checks whether a similar node make any issue other arrangement of nodes. Assuming this is the case, its position becomes augmented. On proceeding with this, the framework will get a bunch of nodes that makes clashes the network with a particular weight or rank.

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. RESULT AND DISCUSSION

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.

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

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.

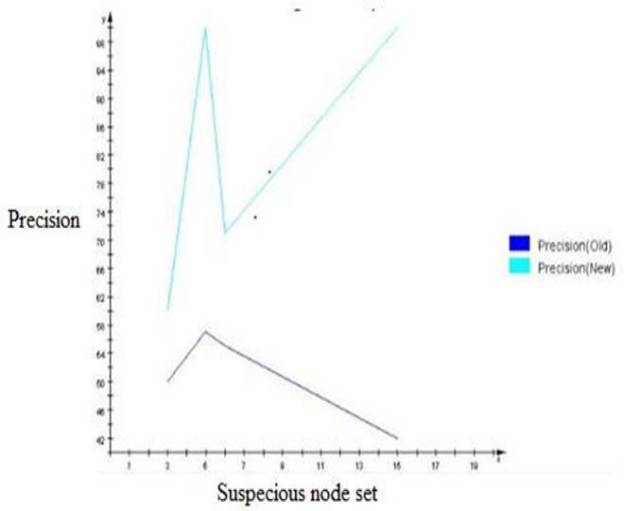

Figure 2: Precision Graph

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.

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.

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.

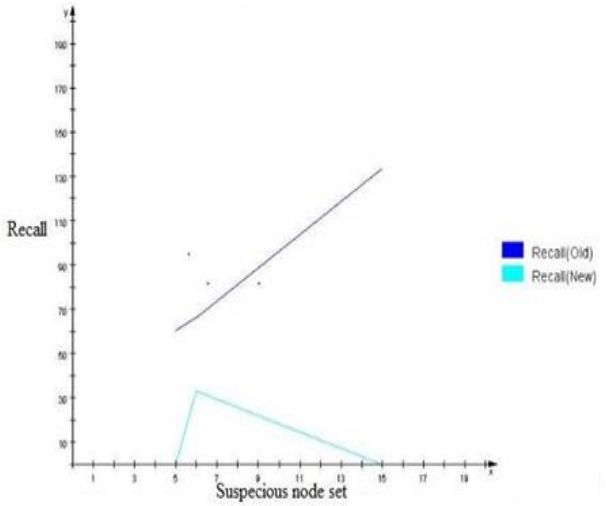

Figure 3: Recall

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

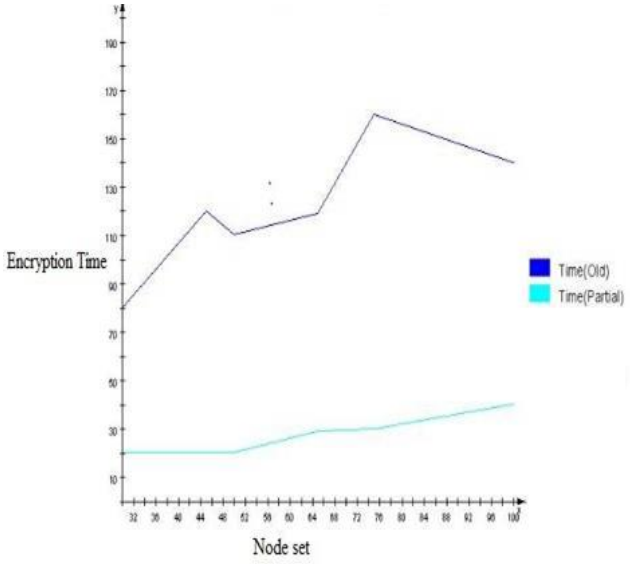

Figure 4: Time Graph

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.

Framework again plays out one more clustering on the chose set of conflict causing nodes. It again isolates the most noteworthy weighted node to one more set. Then dole out new position as 1. Again really takes a look at the isolated nodes s as a chart to recognize the conflict . In the event that recently isolated node again makes any conflict , the framework will augment the node consider 2. By this, framework will again get most separated set that contains the greater part of the fake node.

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.

V CONCLUSION AND FUTURE SCOPE

F measure based vehicular adhoc network assists with distinguishing the false nodes in the framework with further developed accuracy. This structures various groups of nodes and in view of the heaviness of nodes, framework distinguish the misleading hubs. The node set with most elevated weight will be considered as the false nodes in the network. This recognition will require some investment with the assistance of half encryption. Half encryption is a strategy which performs one encryption and twofold decoding. In this manner it lessens the time and builds the security and execution of the framework. F measure based strategy assists with diminishing the review and increment the accuracy for quite a few nodes in the network.

In future, it can utilize various methods to decrease the overhead of the framework by lessening the quantity of messages communicated 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**, Issue **. 6, 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**, Issue **1, 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**, Issue **.6**, **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**, Issue **1**, **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**, Issue **5**, **2011**

[6] 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,pp **2264-2269, 2012.**

[7] Robert K. Schmidtx, Tim Leinm¨ullerx, Elmar Schoch, "*Vehicle Behavior Analysis to Enhance Security in VANETs*", article on telematics and computer networks**, 2014**

AUTHORS PROFILE

Ms.Neethu Maria John Assistant Professor ,Department of Computer Science and Engineering, Mangalam College of Engineering, Kerala, India since 2010.

Ms.Simy Mary Kurian Assistant Professor , Department of Computer Science and Engineering, Mangalam College of Engineering, Kerala, India since 2011.She has completed B.Tech in Computer Science and Engineering from Mahatma Gandhi University and M.Tech in Software Engineering from Karunya Institute of Technology and Science. Her research interest include Image Processing, Data Science, Artificial Intelligence and Bio-inspired Computing .She has associated with many number of undergraduate and research projects.

Dr. Vinodh P Vijayan has completed Bachelors Degree in Electronics and Communication Engineering, Post graduation in Computer Science Engineering and Ph.D in Computer Science & Engineering. He has many years of experience in teaching Undergraduate program and Post graduate programs of M G University and KTU. He was an Adjunct professor for IGNOU post graduate programs and visiting faculty for BITS Pilani's Post Graduate programs He aims to provide innovators with high quality technology information and related services as well as help innovators to create, protect, and manage their intellectual property rights by encouraging them by various motivations .He has served as author/reviewer for many technical publications. His research area includes Soft Computing, AI, Bio-inspired computing, Computer Networks, IoT etc.

Ms.Neema George Assistant Professor, Department of Computer Science and Engineering, Mangalam College of Engineering, Kerala, India since 2008. Her research interest include Image Processing, Data Science, Artificial Intelligence and Cloud Computing. She has associated with many number of undergraduate and research projects.

.

.

