International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

CLUSTER-BASED VANET-ORIENTED EVOLVING GRAPH (CVOEG) MODEL USING GREEDY DETECTION (FLGR)

Mr. Dhamodharan S[1]

[1]Assistant Professor, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, Tamilnadu-624002

Dharani S[2], Deepika R[2], Abinaya D[2]

[2]Department of ECE, SSM Institute of Engineering and Technology, Dindigul, Tamilnadu-624002

Abstract - *Vehicular Ad hoc Networks (VANETs), main objective is to provide road safety and enhance the driving conditions, are exposed to several kinds of attacks such as Denial of Service (DoS) attacks which affect the availability of the underlying services for legitimate users. In vehicular ad hoc networks (VANETs), communication links break more frequently due to the high-speed vehicles. We focus especially on the greedy behavior which has been extensively addressed in the literature for Wireless LAN (WLAN) and for Mobile Ad hoc Networks (MANETs). However, this attack has been much less studied in the context of VANETs. This is mainly because the detection of a greedy behavior is much more difficult for high mobility networks such as VANETs. In this paper, we propose a new detection approach called GDVAN (Greedy Detection for VANETs) for greedy behavior attacks in VANETs. The process to conduct the proposed method mainly consists of two phases, which are namely the suspicion phase and the decision phase. The suspicion phase is based on the linear regression mathematical concept while decision phase is based on a fuzzy logic decision scheme. The proposed algorithm not only detects the existence of a greedy behavior but also establishes a list of the potentially compromised nodes using three newly defined metrics. Moreover, the practical effectiveness and efficiency of the proposed approach are corroborated through simulations and experiments. Our simulation result shows that the proposed scheme significantly outperforms the existing scheme in terms of throughput, delay, energy consumption, cost.*

Key Words: VANET, Greedy detection, linear regression, fuzzy logic.

1. INTRODUCTION

VANET is an application of mobile ad hoc network. More precisely a VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers. Two types of communication are provided in the VANET.

First a pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure. Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle. Each node in VANET is equipped with two types of unit i.e. On Board Unit and Application Unit (AU). OBU has the communicational capability whereas AU executes the program making OBU's communicational capabilities. An RSU can be attached to the infrastructure network which is connected to the Interne. Figure 1 describes C2C-CC architecture of VANET.

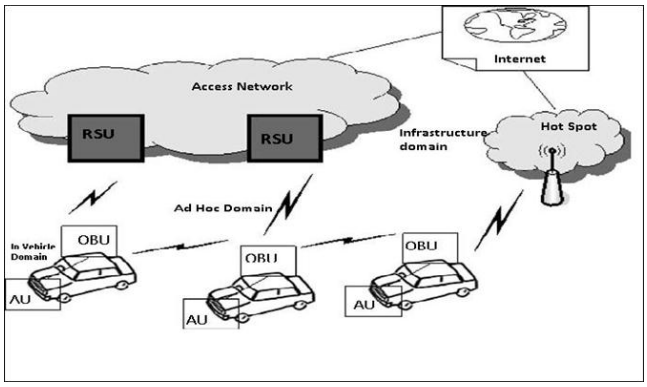

Figure 1. C2C-CC reference architecture

To establish a VANET, IEEE has defined the standard 802.11p or 802.16 (WiMax). A Dedicated Short Range Communication (DSRC) is proposed which is operating on 5.9GHz band and uses 802.11 access methods. It is standardized as 802.11p which provides short range communication with low latency. USA has allocated 75MHz of spectrum in the 5.9GHz band for DSRC to be used by Intelligent Transportation Systems (ITS). Also, Europe has allocated 30 MHz of spectrum in the 5.9GHz band for ITS. In vehicular ad hoc networks (VANETs), communication links break more frequently due to the high-speed vehicles. In this paper, a novel cluster-based VANET oriented evolving graph (CVoEG) model is proposed by extending the existing VoEG model to improve the reliability of vehicular communications[1]. The optimal parameter setting of the optimized link state routing (OLSR), which is a well-known mobile ad hoc network routing protocol, by defining an optimization problem[2].

Some protocols are being developed by the other groups also. NOW (Network on Wheels), which is associated with Car-2-Car Consortium, has developed some protocols. Ford and General Motors have also created a Crash Avoidance Metric Partnership (CAMP) in order to improve the VANET services.

The ultimate goal of all works toward VANET is to provide road safety information among the nodes hence the frequent exchange of such type of data on the network clearly signifies the role of the security. Any successful attack can cause loss of lives or financial lose. Hence the security of the information in VANET is crucial. In this article we are going to discuss the security challenges and major attacks on VANET and also discuss the existing solution for these attacks.

2. PROPOSED METHOD

Vehicular Ad Hoc Networks (VANETs) have received increasing attention from the research and industrial communities recently many valuable applications such as entertainments, Congestion Control, and accident avoidance have been envisioned or planned in VANETs. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) are two major types of communications in VANET. VANETs allow vehicles to connect to roadside units (RSUs), which are fixed infrastructure that are equipped with powerful computing devices and installed at different locations in a city. They can connect with each other via a wired network and with passing by vehicles through wireless communications. Each vehicle equipped with an On Board Unit (OBU) can either transmit hop by hop to the destination using V2V communication or transmit to a Roadside Unit (RSU) using V2I will be possible directly when in range, or across multiple hops. Such hybrid design is very important to realize various types of applications. The design of a system able to monitor the drowsiness level of a driver in an ordinary vehicle is presented. In which the environment can continuously monitor what's happening in it and vehicles can communicate each other exchanging its relative positions and potentially dangerous conditions, such as the presence of an uncontrolled vehicle. As we know large numbers of automobile accidents are caused due to driver fatigue, to address this problem we are proposing a clustering technique which uses V2V communication. The system includes driver fatigue detection System to avoid accident.

We propose a new detection approach called GDVAN (Greedy Detection for VANETs) for greedy behavior attacks in VANETs. The process to conduct the proposed method mainly consists of two phases, which are namely the suspicion phase and the decision phase. The suspicion phase is based on linear regression mathematical concept while decision phase is based on a fuzzy logic decision scheme. The proposed algorithm not only detects the existence of a greedy behavior but also establishes a list of the potentially compromised nodes using three newly defined metrics

The main goal of our algorithm is to supervise the VANET. If a greedy behavior is suspected, the watchdog software determines the responsible nodes using three newly defined metrics. We identify these metrics to be suitable to greedy behavior in VANETs and after a deep study of the 802.11p MAC layer. In fact, according to several studies related to MANETs(Mobile Ad hoc Networks) [6] and [5], the packet delivery ratio, the queue length, the throughput and the backoff supervision can be used as metrics. However, these metrics are only efficient in the case of infra structured or low mobility networks. In the VANET context, due to the high mobility of nodes and their short connection periods, we have argued that it is not practical to use the aforementioned metrics. We have chosen to supervise the number of connection attempts, the node connection durations and the average of waiting times between connections. In fact, a VANET greedy node has not enough time to perform adaptive manipulation of backoff parameters. Another characteristics that it tries to connect to the network more often than honest nodes, also it maintains the medium much more time for its own profit and of course it has to reduce its waiting time between connections.

2.1GDVAN suspicion phase

In a VANET, the nodes of the same WIBSS (Wave Independent Basic Service Set) share access to the transmission medium with respect to CSMA/CA access method managed by the MAC layer protocol which guaranteed a fairness access to all connected nodes. It was observed that for MANET the access times of active nodes are highly correlated. In a normal behavior of the network nodes (without greedy nodes), if the node N1 connects to the support, the node N2 has to wait and cannot connect until N1 ends its transmission. Thus, the connection time of the node Ni+1 linearly depends on connection time of the node Ni. The presence of one or more greedy nodes in the network violates this important access regulation rule.

Correlation coefficient

The correlation coefficient _ measures statistical relationships between two random variables or observed data values. It is defined as the covariance of the variables X and Y divided by the product of their standard deviations.

$$\rho = \frac{Cov(X,Y)}{\sigma_x \sigma_y}$$

To calculate and by definition, it is assumed that the values taken by connection times are random. Statistically, we define the two random variables X and Y as follows: If a node connects to the network at time tn the next connects to time tn+1. Thus X takes values in the set f xi g of the connection times ti of any network node, while Y in the set f yi g of the connection times ti+1. In the case of presence of correlation, the variables xi and yi represent respectively ti and ti+1, which can be connected by a linear relationship.

Thus, our software monitors the following parameters: 1) The duration between two successive transmissions: The waiting time of a greedy node is almost close to zero.2) Transmission time: a greedy node occupies the medium more than other normal nodes.3) Connection attempts number of a node: a greedy node tries much more than the

other nodes to connect to the network. Other parameters can be monitored but for a high efficiency, rapidity and in order to simplify watchdog supervision tool, we have only maintained these parameters.

2.2GDVAN decision phase

For decision making systems, where the membership of an element (node in our case) to a class (honest or greedy) remains proportional, fuzzy logic can be an efficient tool for design. In this work, we propose a new decision scheme for detecting greedy behavior suitable for VANETs. This scheme detects nodes which aim to violate the proper use of the CSMA/CA protocol rules in order to increase their bandwidth at the expense of the well-behaving nodes. It used newly defined metrics which best convenient to highly mobile networks and can be used during short monitoring periods. Design details are given in the following.

As already explained, in our watchdog detection software, we have to supervise the following 3 newly defined metrics for each node in the VANET:

- The Number of connection attempts,

- The average of connection duration,

- The average of waiting times between connections.

From a fuzzy logic point of view, and for each parameter, we begin to suspect the existence of a greedy behavior from a certain value of the parameter (first threshold). Reaching a certain value of the parameter (second threshold) makes suspicion high enough. Between these two threshold values suspicion is gradual. So, our idea is based on the use of the tools provided by the fuzzy logic theory which help to solve this kind of problems.

Before detailing our scheme and the use of the three monitoring parameters, we introduce some basic facts about the fuzzy logic. It helps to understand some basics such as inputs, fuzzy sets, membership functions, inference and defuzzification (for more details refer Inputs, fuzzy sets and membership functions)

As any system of data processing, our fuzzy logic-based scheme requires inputs to be processed to get results. We use the three inputs already described and supervised by the watchdog software after short collection periods. In a high mobility environment such as VANET, we have argued that these tree variables are the most accurate for suspecting a greedy behavior unlike other parameters used for MANET networks for example.

In the classical theory of sets, an element belongs or does not belong to a set. However, this basic concept does not satisfy some simple situations frequently encountered. By contrast, fuzzy set theory permits the gradual assessment of the membership of elements in a set. In this theory, each element belongs partially and gradually to defined fuzzy sets. The contours of each fuzzy set are not ”net”, but ”fuzzy” or” gradual”. This can be described with membership function which takes values in the interval [0; 1], while the indicator of classical function sets takes only 0 or 1. The fuzzy set theory is widely used in a domain where information is incomplete or imprecise.

The designer of a fuzzy logic based system has to clearly define his fuzzy sets. A fuzzy set is defined by its” membership function”, which corresponds to the notion of” characteristic function” in classical logic theory.

Fuzzification step (or the determination of membership degree)is used to switch from real to fuzzy domain. It consists in determining the degree of membership of a input value(measured for example) to a fuzzy set. In our system, for each value of an input variable, we define its membership to one of the following chosen fuzzy sets "Low", "Medium" and "High", respectively denoted by L, M and H.

2.3. SOFTWARE

NETWORK SIMULATOR

A network simulator is a piece of software or hardware that predicts the behavior of a network, without an actual network being present. The network simulator is the program in charge of calculating how the network would behave. Such software may be distributed in source form (software) or packaged in the form of a dedicated hardware appliance. Users can then customize the simulator to fulfill their specific analysis needs. Simulators typically come with support for the most popular protocols in use today, such as IPv4, IPv6, UDP, and TCP.

All the simulation experiments were performed using network simulator NS2.Ns or the Network simulator(also popularly called ns-2) is a discrete event network simulator. It is popular in academia for its extensibility(due to its open source model) and plentiful online documentation. Ns is popularly used in the simulation of routing and multicast protocols, among others, and is heavily used in ad-hoc networking research. Ns supports an array of popular network protocols, offering simulation results for wired and wireless networks alike. It can be also used as limited – functionality network emulator. Ns is licensed for use under version 2 of the GNU General Public License.

3. RESULTS:

Most network simulators use discrete event simulation, in which a list of pending “events” is stored0, and those events are processed in order, with some events triggering future events—such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node. Some network simulation problems, notably those relying on queueing theory, are well suited to Markov chain simulation in which no list of future events is maintained and the simulation consists of transiting between different system “states” in a memoryless fashion . Markov

chain simulation is typically faster but less accurate and flexible then detailed discrete event simulation. Some simulation a are cyclic based simulations and these are faster as compared to event based simulations. Simulation of networks can be a difficult task.

To measure the importance of the proposed protocol, four performance metrics are selected as given below

1)Throughput: It represent the amount of data successfully transferred from source to destination vehicle in a given period of time which is typically measured in kilobits per second(kpbs). Throughput increases of about 21 percent.

2) delay: It refer to the time taken for a packet to be send through the transmission media from the source to destination vehicle. It decreases delay of about 48% when compared to existing algorithm.

3)Energy consumption: It refer to the average rate of the power consumption of node times the time operation. The power consumed in the communication transceiver. It has a lower average of energy consumption of about 37 percent.

4) Workload : It refers to the amount of work done by node or of processing time expected. Figure3.2 shows the workload obtained from simulation. On an average workload in decreases of about 24 percent.

5) Figure 3.1 shows the false positive rate vs cost. When the false positive error increases the bit per item decreases. The error is decreases of about 24 percent.

CVoEG is specially designed for the highly evolving traffic scenarios. The cluster maintaining cost of both schemes are shown in fig. CVoEG with FLGR is more stable as compared to the CEG-RAODV in the context of throughput. The more suitable route will be selected from source to destination. The proposed scheme perform better than other existing scheme. The simulation shows that the proposed scheme achieves good throughput, end to end as compared with CEG-RAODV, EG-RAODV.

Fig 3.1 Impact of FPR on Bits per element

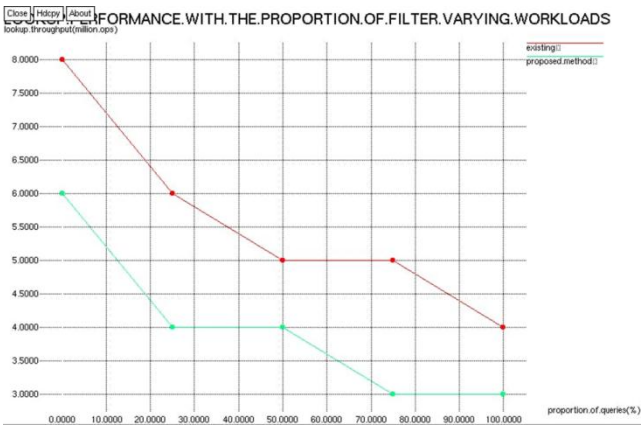

Fig 3.2 Impact on workload

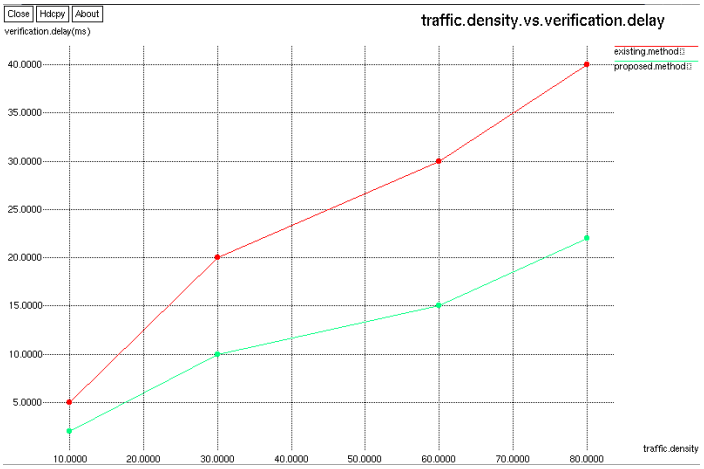

Fig 3.3 Impact of traffic density on verification delay

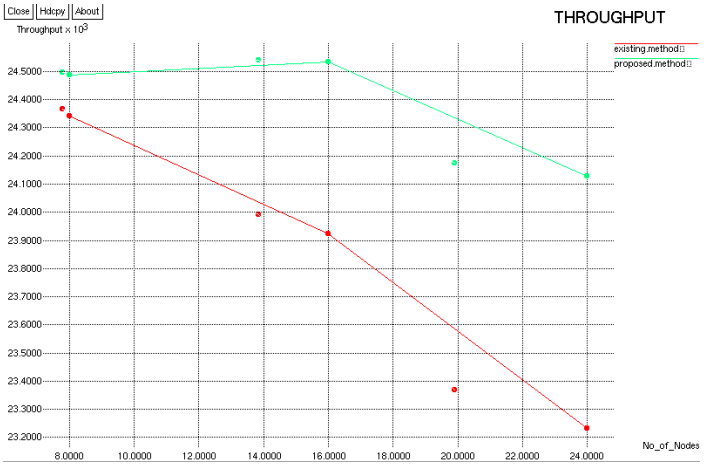

Fig 3.4 Impact on no. of node on throughput

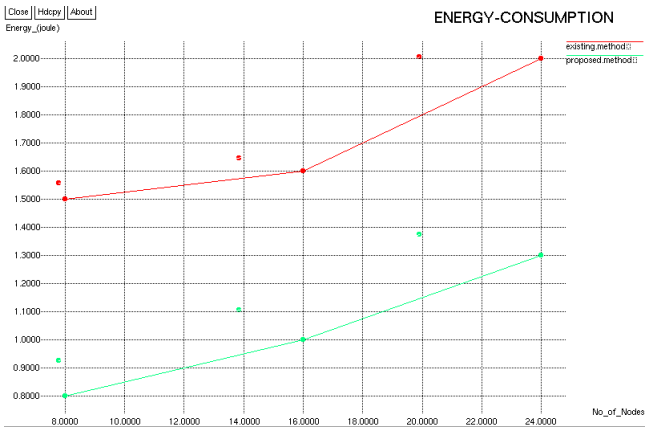

Fig 3.5 Impact on no. of node on energy

The reason behind the excellence performance is the adaptation of the CVoEG model. It significantly reduces the time complexity. The proposed model easily extendable to a new reliable routing scheme by integrating the proposed CVoEG model and FLGR routing scheme. The new FLGR routing scheme performs very well on traffic scenarios with varying vehicular speeds. Resulting in the 30% to 40% improvement in all performance metrics, i.e. throughput, end to end delay, energy consumption. The impact of different speeds, packet sizes and transmission range are significant compared to the existing schemes in the literature.

4. CONCLUSION:

We propose in this paper GDVAN (Greedy Detection for VANETs): A new algorithm for detecting greedy behavior in VANETs. GDVAN uses three newly defined metrics which were argued to be well appropriate for greedy detection in a high mobile environment such as VANET, where connections are short and nodes have not enough time to perform adaptive manipulation of back off parameters. It is composed of both suspicion and decision phases respectively based on enhanced linear regression and fuzzy logic concepts. By monitoring network traffic traces, the algorithm is able to affirm the existence or not of a greedy nodes. In the affirmative case, it is able also to determine responsible nodes. GDVAN has the advantages of being passive, nonrecourse-intensive and does not require changes in MAC layer. It has the advantage also to be transparent to users and it can be executed by any node of the network. The simulation results are quite promising and they confirmed the correctness of our choice of the metrics and the decision method design.

REFERENCES:

[1]Zahid khan, Pingzhi Fan, Sangsha Fag, Fakhar Abass, "An Unsupervised Cluster- Based VANET-Oriented Evolving Graph (CVoEG) Model and Associated Reliable Routing Scheme" in Intelligent Transportation system., march 2019.

[2] Jamal Toutouh, Jose Garcia-Nieto and Enrique Alba "Intelligent OLSR Routing Protocol Optimization for VANETs", in Vehicular Technology, vol.61, no.4, may 2012.

[3] Albert Wasef, Yixin Jiang and Xuemin Shen," An Efficient Distributed- Certificate- Service Scheme for Vehicular Networks ", in Vehicular Technology, vol. 59,no.2 ,February 2010.

[4] Huixian Wang, Ren Ping Liu, Wei Ni and Iain B. Collings," VANET Modeling and clustering Design under practical Traffic, Channel and Mobility Conditions", in Communication,vol.63,no.3,2015.

[5] SuKyoung Lee, Kotikalapudi Sriram, Kyungsoo Kim,Yoon Hyuk Kim and Nada Golmie," Vertical Handoff Decision Algorithms for providing Optimized Performance in Heterogeneous Wireless Networks", in Vehicular Technology,vol.,58,no.2, February 2009.

[6]Ming-Chin Chuang and Meng Chang Chen , "DEEP: Density-Aware Emergency Message Extension Protocol for VANETs" in wireless communication , vol.,12, No.10, October 2013.

[7] Ammara Anjum Khan, Mehran Abolhasan, Wei Ni, Justin Lipman and Abbas Jamalipour," A Hybrid-Fuzzy Logic Guided Genetic Algorithm (H-FLGA) Approach for Resource Optimization in 5G VANETs A Hybrid-Fuzzy Logic Guided Genetic Algorithm" in Vehicular Technology,vol.68,no.7,July 2019.

[8] Yi Zhou, Huanhuan Li, Chenhao Shi, Ning Lu and Nan Cheng, "A Fuzzy-Rule Based Data Delivery Scheme in VANETs with Intelligent Speed Prediction and Relay Selection", in Wireless Communications and Mobile Computing,vol.,10,2018.

[9]Siddhartha B S, Sunil Kumar B R, Arpitha K, Shwetha S N, "Routing Protocol using Fuzzy Logic for Vehicular Ad-Hoc Networks" in Technology and Engineering,vol.,8 no.2,july 2019.

[10]F.Azzali, O.Ghazali, M.H.Omar "Fuzzy Logic based Intelligent Scheme for Enhancing QoS of Vertical Handover Decision in Vehicular Ad-hoc Networks" in material science and engineering in 2017.