Fuzzy Based Attack Detection Algorithm For Vanet

M. Vaitheki, Ms. L. Rachel
[1]*M.E student* , [2]*Assistant professor/ECE*
Chandy Engineering College, Mullakkadu,Tuticorin - 628005

ABSTRACT

Vehicular Ad hoc networks (VANET) are a key element of cooperative intelligent transport systems. One of the challenges in VANETs is dealing with awareness and congestion due to the high amount of messages received from the vehicles in communication range In this project, Propose a novel GDVAN for Emergency Data (FSWTMED) in vehicular ad hoc net-works, 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.NS2 tool has been used to evaluate a performance of existing and proposed system

I. INTRODUCTION

In a Vehicular Ad hoc Network (VANET), vehicles communicate with each other through Dedicated Short Range Communication (DSRC) wireless devices. Equipped with hundreds of smart sensors, vehicles can detect their own moving status (such as braking, lane changes, and acceleration) and road conditions (such as icy roads and weather conditions).

VANET enables a large number of interesting applications, and the major goal is to improve road safety and transportation efficiency by exchanging data between vehicles. Toward the goal of efficient design of VANETs, the aim of this paper is to develop a method that will allow the estimation of the time for which an existing route will continue to operate satisfactorily, which is defined as the route residual time (RRT), and demonstrate how such a method may be integrated in routing protocols. For the route to continue to be valid for a given period of time, all the individual links comprising the route need to continue to be available. In other words, the lifetime of a route is determined by the lifetime of its "weakest" link. A wireless link on the VANET context will be available until the channel quality deteriorates so much that it drops below a given communication threshold. This reduces the problem of estimating RRT to the estimation of the remaining time for which a link's quality will remain above the specified threshold, which is defined as the link residual time (LRT).

The importance of plotting the nonrandom behavior of the nodes' mobility patterns to construct long-lived routes and combat frequent communication disconnections was established in [2], where the authors propose the utilization and dissemination of GPS information to calculate the expected connection duration and demonstrate significant performance enhancement when the routing procedure provisionally takes lifetime into account.

II. RELATED WORK

The problem of routing through paths of higher lifetime, which entails the estimation of the links' lifetimes and the routing decision process, has been the topic of several recent studies. As far as the link lifetime estimation methods are concerned, related studies can largely be divided into three categories: 1) methods that assume knowledge of the other nodes' positions and velocity vectors (such as [2], [7], [8], or [9]); 2) analytical methods based on the extraction of lifetime distributions (such as [10] or [11]); and 3) methods that make use of some link quality metric (such as [12]–[16] or [17])

In general, methods of the first category require use of additional equipment, whereas the transmission range of the nodes is considered deterministic and known a priori, assuming a free space propagation model and a fixed known value of transmission power. However, being within range, as this isspecified based on this assumption, does not always guarantee radio connectivity, particularly in an urban environment. The methods proposed here include transmission power as a parameter, which is to be estimated by the methods themselves. Moreover, the information acquired via GPS might be inaccurate. Methods targeting at analytically extracting link lifetime distributions naturally operate under the assumption of specific mobility models, such as the random waypoint model, and are thus applicable

only to these cases when the vehicles follow the mobility model, on which the analysis has been based on. Utilizing information related to the quality of the radio link to construct reliable routes offers an immediate way to exploit the direct coupling of physical layer operations to the network topology. There exist approaches, such as [12], [13], or [14], employing the exponentially smoothed value of the received power or SNR of ongoing packets. Such a criterion focuses more on the past observations without extrapolating in the future, and thus implicitly assumes a stable grouping of the nodes, and the existence of neighbors with similar mobility characteristics, which may not always be the case in such a dynamic environment

III. PROPOSED SYSTEM DESIGN

In this project, to obtain the transmission In VANETs, the primary security requirements are identified as entity authentication, message integrity, nonrepudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements. PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long. In Hubaux identify the specific issues of security and privacy challenges in VANETs, and indicate that a PKI should be well deployed to protect the transited messages and to mutually authenticate network entities. In Raya and Hubaux use a classical PKI to provide secure and privacy preserving communications to VANETs. In this approach, each vehicle needs to preload a huge pool of anonymous certificates. The number of the loaded certificates in each vehicle should be large enough to provide security and privacy preservation for a long time, e.g., one year. Each vehicle can update its certificates from a central authority during the annual inspection of the vehicle. In this approach, revoking one vehicle implies revoking the huge number of certificates loaded in it. , Studer et al. propose an efficient only within the coverage range of the RA. It should be noted that TACK requires the RAs to wait for some time, e.g., 2 seconds, before sending the new certificate to the requesting vehicle. This renders the vehicle not able to send messages to neighboring vehicles within this period, which makes TACK not suitable for the safety applications in VANETs as the WAVE standard requires each vehicle to transmit beacons about its location, speed, and direction every 100-300 msec. Also, TACK requires the RAs to completely cover the network, otherwise, the TACK technique may not function properly.

This requirement may not be especially in the early deployment stages of VANETs. Although TACK eliminates the CRL at the vehicles level, it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates. To check the revocation status of a vehicle, the RA has to verify that this vehicle is not in the current RL by preforming a check against all the entries in the RL. Each check requires three pairing operations. Consequently, checking the revocation status of a vehicle may be a time consuming process. The authors suggested to use an optimized search method to remedy the computationally expensive RL check. The proposed method can reduce the RL checking to two pairing operations. However, this solution is based on fixing some parameters in the group signature attached to every certificate request, which reduces the privacy preservation of TACK and renders the tracking of a vehicle possible. There are some works addressing the problem of distributing the large-size CRL in VANETs.

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 withpowerful 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 dangerousconditions,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 behaviorin 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 supervisioncan be used as metrics. However, these metrics are only efficient in the case of infrastructured or low mobility networks. In the VANET context, due to the high mobility of nodes and their short connection periods, we have arguedthat 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 VANETgreedy node has not enough time to perform adaptive manipulation of backoff parameters. Another characteristic is 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.

A. GDVAN 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 methodmanaged 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 tothe 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 timesti of any network node, while Y in the set fyi g of the connection times ti+1. In the case of presenceof 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 tozero. 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.

B. GDVAN 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 solvethis 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 MANETnetworks 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 ofthe 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 isincomplete 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.

C. Fuzzification and membership degree

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.

IV – SIMULATION RESULTS

The simulation results are quite promising and they confirmed the correctness of our choice of the metrics and the decision method design. Moreover, the simulation results have demonstrated that GDVAN can improve the packet delivery ratio due to establishing stable routes.

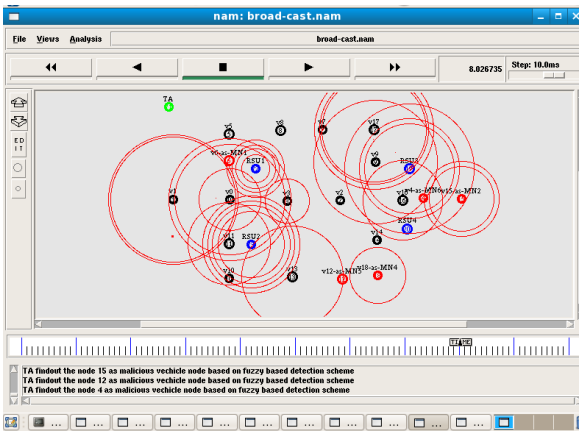

Figure delay measurement

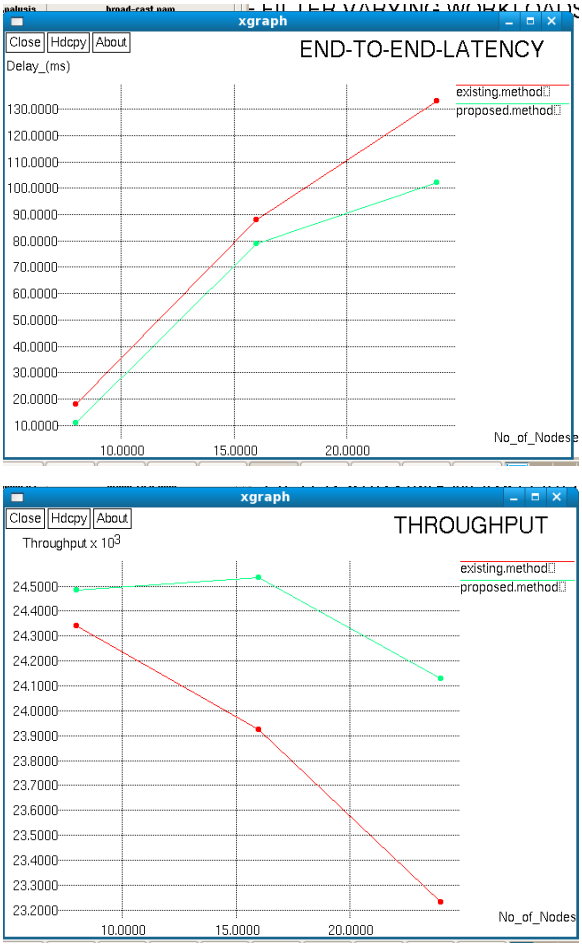

Figure throughput measurement

V - CONCLUSION

To deal with, we propose in this project 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 backoff 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.

REFERENCES

[1]. J. Blum, A. Eskandarian, and L. Hoffman, "Challenges of intervehicle ad hoc networks," IEEE Trans. Intell. Transp. Syst., vol. 5, no. 4, pp. 347– 351, Dec. 2004.

[2]. W. Su, S. J. Lee, and M. Gerla, "Mobility prediction and routing in ad hoc wireless networks," Int. J. Netw. Manage., vol. 11, no. 1, pp. 3–30, Jan./Feb. 2001.

[3]. K. W. Chin, J. Judge, A. Williams, and R. Kermode, "Implementation experience with MANET routing protocols," SIGCOMM Comput. Commun. Rev., vol. 32, no. 5, pp. 49–59, Nov. 2002.

[4]. Z. Cheng and W. B. Heinzelman, "Discovering long lifetime routes in mobile ad hoc networks," Ad Hoc Netw., vol. 6, no. 5, pp. 661–674, Jul. 2008.

[5]. I.Chlamtac, M. Conti, and J. J. N. Liu, "Mobile ad hoc networking: Imperatives and challenges," Ad Hoc Netw., vol. 1, no. 1, pp. 13–64, 2003.

[6]. D. S. J. De Couto, D. Aguayo, B. A. Chambers, and R. Morris, "Performance of multihop wireless networks: Shortest path is not enough," SIGCOMM Comput. Commun. Rev., vol. 33, no. 1, pp. 83–88, Jan. 2003.

[7]. H. Menouar, M. Lenardi, and F. Filali, "Improving proactive routing in VANETs with the MOPR movement prediction framework," in Proc. 7th ITST, Sophia Antipolis, France, 2007, pp. 1–6.

[8]. J. Tang, G. Xue, and W. Zhang, "Reliable ad hoc routing based on mobility prediction," J. Combinatorial Optim., vol. 11, pp. 71–85, Feb. 2006.

[9]. Z. J. Haas and E. Y. Hua, "Residual link lifetime prediction with limited information input in mobile ad hoc networks," in Proc. IEEE INFOCOM, 2008, pp. 1867–1875.

[10]. Y. C. Tseng, Y. F. Li, and Y. C. Chang, "On route lifetime in multihop mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 4, pp. 366–376, Oct.–Dec. 2003.

[11]. S. Jiang, D. He, and J. Rao, "A prediction-based link availability estimation for mobile ad hoc networks," in Proc. IEEE INFOCOM, 2001, pp. 1745–1752.

[12]. R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tripathi, "Signal stability based adaptive routing for ad-hoc mobile networks," IEEE Pers. Commun., vol. 4, no. 1, pp. 36–45, Feb. 1997.

[13]. C. K. Toh, "Associativity-based routing for ad-hoc mobile networks," Wirel. Pers. Commun., vol. 4, no. 2, pp. 103–139, Mar. 1997.

[14]. H. M. Tsai, N. Wisitpongphan, and O. Tonguz, "Link-quality aware ad hoc on-demand distance vector routing protocol," in Proc. 1st Int. Symp. Wirel. Pervasive Comput., Jan. 2006, pp. 1–6.

[15]. J. Singh, N. Bambos, B. Srinivasan, D. Clawin, and Y. Yan, "Proposal and demonstration of link connectivity assessment based enhancements to routing in mobile ad-hoc networks," in Proc. IEEE 58th Veh. Technol. Conf., 2003, vol. 5, pp. 2834–2838.

[16]. S. Agarwal, A. Ahuja, J. P. Singh, and R. Shorey, "Route-lifetime assessment based routing (RABR) protocol for mobile ad-hoc networks," in Proc. IEEE ICC, 2000, vol. 3, pp. 1697–1701