VOL. 12, NO. 1, JANUARY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

CLASSIFYING MALICIOUS NODES IN VANETS USING SUPPORT VECTOR MACHINES WITH MODIFIED FADING MEMORY

S. Sharanya[1] and S. Karthikeyan[2]
[1]Department of Computer Science and Engineering, SRM University, Kancheepuram, Tamil Nadu, India
[2]Department of Automobile Engineering, B.S. Abdur Rahman University, Vandalur, India
E-Mail: sharanya.se@ktr.srmuniv.ac.in

ABSTRACT

Vehicular Adhoc Networks (VANETs) gain more attention in the modern world. The advancements in telecommunication technology has opened the door for deploying VANETs to make the roadway journey a more safer and comfortable one. The challenges such as mobility, network scalability and volatility make the VANETs more prone to be attacked by the intruders. In an open medium like VANETs, identifying the intruder is a difficult task. The behaviour of intruders or malicious users is studied using various machine learning techniques. The work focuses on applying Support Vector Machine (SVM), a semi-supervised learning algorithm with Modified Fading Memory for predicting the behaviour of the users of VANETs (SVM-MFM) and classifying the intruders from users of the network. This classification helps to isolate the intruders and the communication of the intruder with the VANET can be stopped, thus providing better resource utilization. This scheme is computationally fast in classifying the intruders with high ROCC of 98%.

Keywords: VANETs, support vector machines, fading memory, support vector machines-modified fading memory (SVM-MFM).

1. INTRODUCTION

Vehicular Adhoc Networks (VANETs) are very special type of Mobile Adhoc Networks (MANETs) in which the vehicles behave as mobile nodes, thus forming a vehicular network [1]. The basic idea is to provide connectivity to the road users through vehicle-to-vehicle communications thus forming the Intelligent Transportation Systems (ITS). The major services offered by the ITS are traffic and accident monitoring, providing real time information and infotainment. VANETs operate in an open wireless medium in adhoc fashion giving room to numerous challenges to be addressed in their set up. The physical infrastructure of VANETs consists of two main components namely Road Side Units (RSU) and On Board Unit (OBU). The RSU function as a router and OBUis responsible for communicating the messages with the vehicles in vicinity. Figure-1 shows the typical communication scenario of VANET. The communication standards adopted in VANETs are Dedicated Short Range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE) (IEEE 1609.11p) [2].

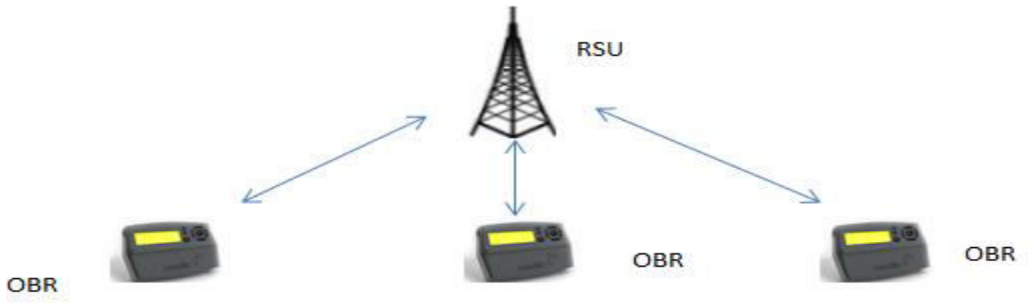

Figure-1. VANET Scenario.

VANETs operate in open wireless medium and hence have unique issues and security threats. Defending nodes of the VANET from the attackers is a challenging task. Identifying the malicious node from a dynamically changing network requires continuous monitoring and recording of the all the communications between the nodes in a VANET, which is practically difficult to achieve. The main objectives of this paper is to exploit the spatial reusability in deploying the Support Vector Machines with Modified Fading Memory (SVM-MFM) that tracks the communications between the nodes only for limited time and thus classify a node either as malicious node or legitimate node [18]. After a node is classified as a malicious node, the further communications from that node can be disrupted, thus saving network resources.

This work is organised as follows. Section 2 presents the issues in VANETs. Section 3 summarizes the related work. Section 4 describes the proposed SVM-FM. Section 5 presents the evaluation and Section 6 concludes the paper with future work.

2. CHALLENGES IN VANETS

Though VANETs are specialized form of MANETs, they have unique issues to be addressed. Some of the major issues are listed below [3] [13] [16]:

- No central controlling authority
- Heterogeneous network
- In-securedwireless medium
- Lack of proper data management and storage facilities
- Fragmented network
- Varying network density
- Difficult to track a node
- Physical constraints on the road
- Geographical communication

3. RELATED WORKS

The last few decades saw dramatic development in the Intelligent Transportation System (ITS) to improve the road safety. The primary goals of ITS are improved road safety, accident notification, road hazard notification, traffic monitoring, remote vehicle diagnosis, and infotainment. Extensive research has been done in the field of VANETs to enhance the security.

Joyti *et al*. classified a node as malicious node using both binary and multi class classification [4]. The classification is based on the features such as speed deviation of the node, strength of the received signal and packet delivery ratio. In binary classification a node is classified either as a malicious node or a legitimate node. In multi class classification, a malicious node is classified into one of the misbehaving classes.

Joyti *et al* classified a node based on ensemble machine learning approach [5]. In this work, the benefits of different classification techniques are combined using ensemble approach to achieve high degree of correct classification.

Uzma Khan proposed an algorithm that effectively selects proper verifiers for malicious node detection [6]. A node is marked as malicious node based on the packet drop and delivery ratio. Ashish Vulimiri verified the reliability of the primary alerts by investigating the correlated secondary information [7]. The secondary information is collected from multiple sources to generate the degree of belief from which the truthfulness of the alert message is derived.

Chil-Hwa Kim framed a Misbehaviour Based Repudiation Management System (MBRMS) that efficiently detects the misbehaviour, broadcasts the events and also filters the false data using outlier detection method [8]. The node's misbehaviour is predicted based on the node risk value.

Sandeep K.Harit designed Fox-hole model of Misbehaviour detection, a data centric approach to check whether the information received is genuine [9]. The misbehaving node is detected by measuring the truth-value of the broadcasted alert messages. Rehan Akbani *et al*., used Fading Memories to track the communications in a longer time frame and tried to extract data only with few features [10]. The accuracy was improved using dynamic thresholds with low computational overhead.

The above works focus on detecting the misbehaviour of nodes based on the messages generated by the nodes. Tracking the messages of all the nodes of the VANET for long time period is tiresome. The dynamic topology of the VANET could be exploited for reutilization, signal strength of the resources so that every node of the VANET could be monitored only for fixed time limit.

4. PROPOSED WORK

The proposed classification scheme considers the following critical parameters to classify a node as malicious node namely power ratio, signal strength, packet delivery ratio, speed of node, number of packets generated and transmission power. The spatial reusability of the VANETs is exploited in monitoring the node only for a particular time period. The SVM-MFM has two phases namely pre-processing phase and classification phase as given in Figure-2.

A) Pre-processing phase

This phase determines the range of nodes for tracking the communication factors mentioned above. Since the nodes (vehicles) move fast in the network, it is not necessary to track and maintain the information of the nodes that have left the network. The spatial reusability-aware single-path routing protocol (SASR) is used to obtain the information about the nodes existence and connectivity inside the network [11] [15]. Only the nodes that are actively communicating are allowed for proceeding to the next phase. A node is discarded from the classification, if it neither sends nor responds to any of the probes/ messages sent by the RSU for a fixed time period. The nodes that exhibit poor communication within the network need not be monitored, thus implementing the Modified Fading Memory (MFM). The time interval to decide about the node's participation is chosen based on the network density.

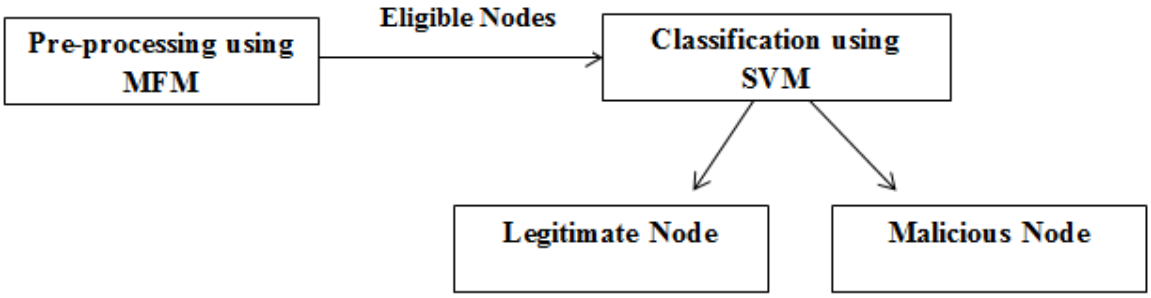

Figure-2. Overview of SVM-MFM.

B. Classification phase

The classification of a node as malicious node or legitimate node is done using Support Vector Machines (SVM), a semi supervised learning algorithm [12]. The training to this algorithm is provided by the truth value which is obtained by calculating the Weighted Trust Factor (WTF (t)) of the critical factors at time t. The factors are measured once in t seconds for time duration of T minutes. WTF (t) is determined using the following expression [13]:

$$WTF(t)=\sum_{n=1}^{N} W_n(t) U_n(t) \quad (1)$$

WTF(t) is the weighted trust factor calculated from the product of weightage (W(t)) and parameters (U(t)) at a time instance t. The WTF (t) is used to train the SVM parameter to predict a node's behaviour at a time instance t+1.

The novelty of the proposed work is that the Modified Fading Memory (MFM) exploits the idea of spatial reusability within the VANET. The SVM-MFM do not consider the nodes which are out of range of the VANET communication both in terms of time and space.When the node is not within the range of the RSU, its communication capacity will gradually decrease. So these nodes need not be monitored, thus reducing the computational overhead. Figure 3 shows the methodology of SVM-MFM.

The Support Vector Machines-Fading Memory (SVM-FM) [10] tracks the nodes movement and communication for longer period of time. This method gives accurate classification at the cost of high computational time. This method also demands the maintenance of database of the network parameters that were monitored in longer range. This is an overhead to the RSU. The SVM-MFM presents a feasible solution to the above mentioned issues by considering the nodes which exhibit good communication quality only for particular time period. The SVM-MFM is well suited for VANETs because the nodes or vehicles under the surveillance of RSU moves very fast and fades away from the range. Hence the RSU need not track it for longer time.

5. EVALUATION

The classification of malicious nodes and legitimate node using SVM-MFM is shown in figure 4. The SVM-MFM linear hyper-plane equations are [12]:

wx + b>=0 for legitimate node
wx + b<0 for malicious node

The WTF (t) is calculated for a time interval t=2 seconds for the time duration of T=2 minutes. The parameters namely power ratio, signal strength, packet delivery ratio, speed of node, number of packets generated and transmission power were measured for 50 VANET nodes. The modified fading memory time threshold fixed here was 2 minutes.

A) Evaluation metrics

The SVM-MFM is tested for two primary factors namely: Rate of Correct Classification (ROCC) and computational complexity. VANETs are time critical application, thus they demand fast processing. So algorithms that yield accurate result in minimum time are very vital in VANETs.

The ROCC is calculated from the following expression [13]:

$$ROCC= (a+d) * 100/n \quad (2)$$

where a is the actual positive value and d is actual negative value over n samples. ROCC is a good factor to determine the performance of the classification algorithms. The SVM-MFM shows the ROCC of 98% and the classification is shown in Figure-4.

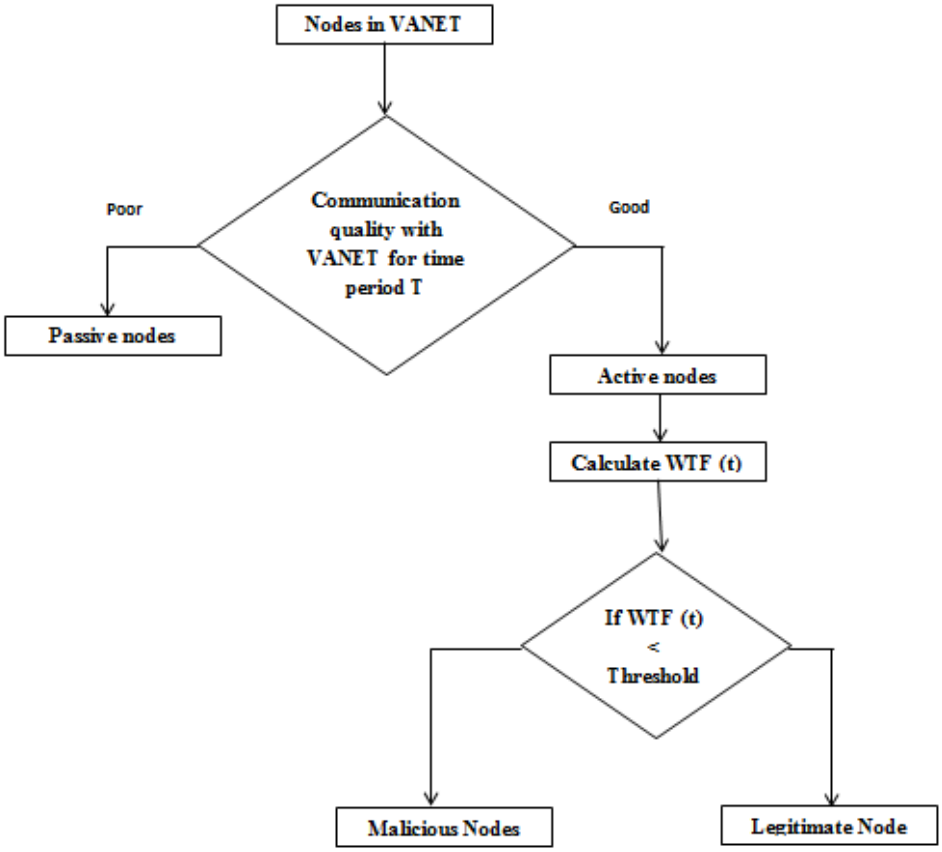

Figure-3. Working of SVM-MFM.

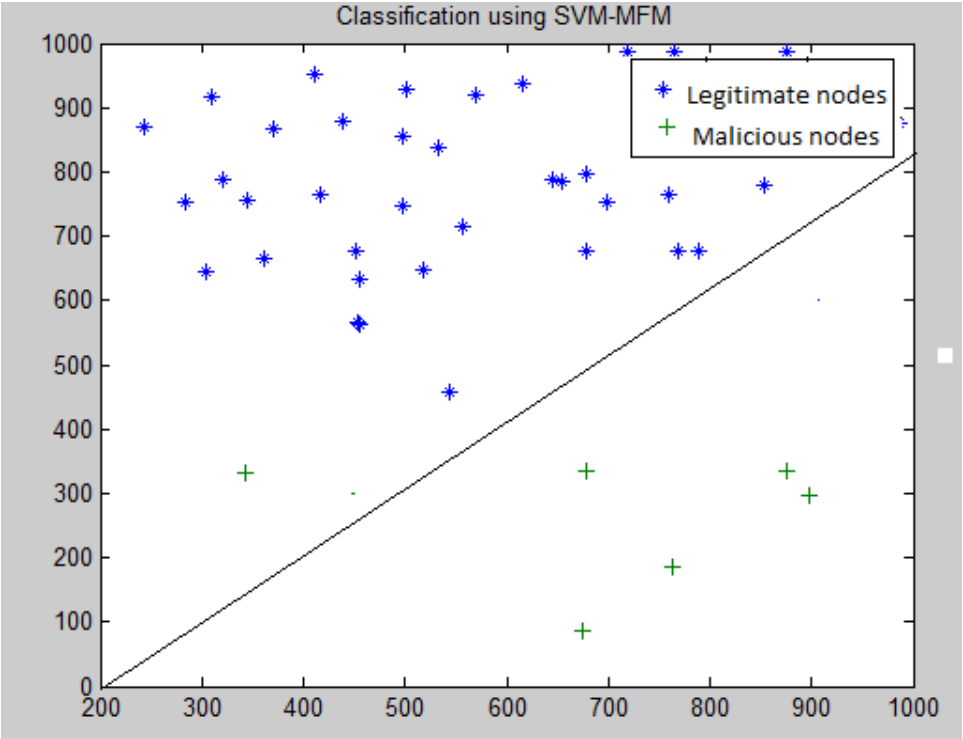

Figure-4. Classification of malicious nodes and legitimate node using SVM-MFM.

The SVM-MFM is fast in classifying a node as legitimate or malicious node. SVM-MFM exhibits half the computational time than the earlier classification schemes namely SVM with fading memory or SVM without fading memory. This is shown in Figure-5.

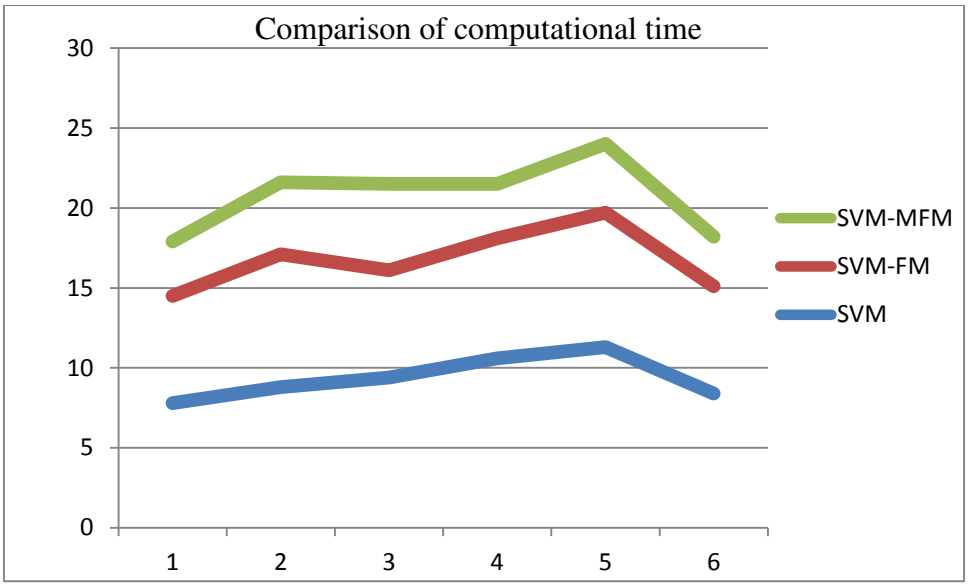

Figure-5. Comparison of computational time.

6. CONCLUSION AND FUTURE WORK

The proposed SVM-MFM classifies the VANET nodes into malicious and legitimate nodes so that the further communication through the malicious nodes can be avoided. This can save the network resources and thus avoids the intruder from accessing the data in the network. Predicting the node's behaviour as legitimate or malicious using SVM-MFM will be a proactive measure in preventing the VANET from being hacked. The SVM-MFM has shown good performance over the other two methods SVM-FM and SVM without fading memory in terms of ROCC and computational time. The SVM-MFM is a binary classification model that classifies a node into one of the two classes namely malicious and legitimate. Multiclass classification model can be used to classify the type of attack or attacker in the VANET.

REFERENCES

[1] Marwa Altayeb and Imad Mahgoub. 2013. A Survey of Vehicular Ad hoc Networks Routing Protocols. International Journal of Innovation and Applied Studies, ISSN 2028-9324, 3(3): 829-846.

[2] Lusheng Miao, Karim Djouani. 2011. A Survey of IEEE 802.11p MAC Protocol. Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunication.

[3] Felip e Cunha, Azzedine Boukerche, Leandro Villas, Aline Viana, Antonio A. F. Loureiro. 2014. Data Communication in VANETs: A Survey, Challenges and Applications. Data Communications in VANETs, ISSN 0249-6399.

[4] Jyoti Grover, Nitesh Kumar Prajapathi, Vijay Laxmi, Manoj Singh Gaur. 2011. Machine Learning Approach for Multiple Misbahavious Detection in VANET. Springer-Verlag Berlin. pp. 644-653.

[5] Jyoti Grover, Vijay Laxmi and Manoj Singh Gaur. 2012. Misbehavior Detection Based on Ensemble Learning in VANET. International Conference on Advanced Computing. pp. 602 to 611.

[6] Uzma Khan, Shikha Agrawal, Sanjay Silakari. 2015. Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks. International Conference on Information and Communication Technologies. 46: 965-972.

[7] Ashish Vulimiri, Arobinda Gupta, Pramit Roy, Skanda N. Muthaiah, and Arzad A. Kherani. 2010. Application of Secondary Information for Misbehavior Detection in VANETs. International Federation for Information Processing. pp. 385-396.

[8] Chil-Hwa Kim and Ihn-Han Bae. 2012. A misbehaviour- Based Reputation Management System for VANETs. Springer Science.

[9] Sandeep K. Harit, Gaurav Singh, Neeraj Tyagi. 2012. Fox-Hole Model for Data-centric Misbehaviour

Detection in VANETs. IEEE conference on Computer and Communication Technology.

[10] Rehan Akbani, Turgay Korkmaz, G.V. Raju. 2011. EMLTrust: An enhanced Machine Learning based Reputation System for MANETs. Elsevier.

[11] Tong Meng, Fan Wu, Member, Zheng Yang, Member, Guihai Chen, Athanasios V. Vasilakos. 2016. Spatial Reusability-Aware Routing in Multi-Hop Wireless Networks. IEEE transactions on computers. 65(1).

[12] S. Abe. 2010. Support Vector Machines for pattern classification. Advances in Pattern Recognition, 2nd ed., Springer. pp. 2089-2093.

[13] H. Yang, H. Luo, F.Ye, S. Lu, L. Zhang. 2004. Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications. 11(1): 38-47.

[14] T. Jiang, J.S. Baras. 2006. Trust evaluation in anarchy: a case study on autonomous networks. Proceedings of the 25th Conference on Computer Communications, Barcelona, Spain. pp. 23-29.

[15] H. Zhai and Y. Fang. 2006. Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks. In: Proc. IEEE 25th IEEE Int. Conf. Comput. Commun. pp. 1-12.

[16] B. Mishra, P. Nayak, S. Behera, D. Jena. 2011. Security in vehicular adhoc networks:a survey. Proceedings of the 2011 International Conference on Communication, Computing and Security, ACM. pp. 590-595.

[17] J. Luo J.-P. Hubaux. A survey of inter-vehicle communication. Tech. Rep EPFL, Lausanne, Switzerland.

[18] Philippe Golle, Dan Greene, Jessica Staddon. 2004. Detecting and correcting malicious data in VANETs. Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, ACM. pp. 29-37.