International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 7 Issue 9 ǁ 2019 ǁ PP. 13-22

Machine Learning approach in Malicious Node Detection

Trilochan rout, Sidhanta kumar balabantaray, sushree sangita jena,ashis kumar acharya

Department of Computer science and Engineering, NM Institute of Engineering and Technology,Bhubaneswar , Odisha
Department of Computer science and Engineering, Raajdhani Engineering College,Bhubaneswar,Odisha
Department of Computer science and Engineering ,Aryan Institute of Engineering and Technology Bhubnaeswar , Odisha
Department of Computer science and Engineering,Capital Engineering College

ABSTRACT— *Vehicular Ad hoc Networks (VANETs) give successful vehicular activity for wellbeing just as greener and more productive correspondence of vehicles in the Dedicated Short Range Communication (DRSC). The powerful idea of the vehicular organization geography has presented numerous security challenges for successful correspondence among vehicles. Thus, models have been applied in the writing to checkmate the security issues in the vehicular organizations. Existing models need adaptability and adequate usefulness in catching the unique practices of malevolent hubs in the profoundly unstable vehicular correspondence frameworks. Given that current models have neglected to address up with the difficulties engaged with vehicular organization geography, it has gotten basic to receive reciprocal measures to handle the security issues in the framework. The methodology of trust model as for Machine/Deep Learning (ML/DL) is proposed in the paper because of the hole in the territory of organization security by the current models. The proposed model is to give an information driven methodology in settling the security challenges in unique organizations. This model goes past the current works adroitly by demonstrating trust as an order interaction and the extraction of pertinent highlights utilizing a half and half model like Bayesian Neural Network that consolidates profound learning with probabilistic displaying for wise choice and compelling speculation in trust calculation of legitimate and exploitative hubs in the organization.*

I. INTRODUCTION

Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication use Dedicated Short Range Communication (DSRC) technology in Intelligent Transportation Systems (ITS) domain to provide secure and reliable communication links among vehicles and vehicle to infrastructure [1]–[4]. These communication links allow the transfer of data neces- sary for the operation of different ITS applications. DSRC is developed to work in highly dynamic networks, to support fast link establishments and to minimize communication latency. It is mainly designed to ensure service reliability for safety applications. Taking into account the time constraints for these type of applications, DSRC provides robust and periodic updates about their status and events. However, there are drawbacks including low scalability and lack of processing power due to the huge amount of data involved [5]. These limitations call for some complementary measures to establish a secure vehicular network.
Literature shows a significant number of light-weight
authentication algorithms. For example, [5], [6] investigated that these techniques have not been able to provide sufficient protection for connected vehicles (CVs) when authenticated nodes are being compromised in the network.

The communication concerns as a result of the stated short- comings of DRSC, call for more reliable and robust trust approaches in addressing the security issues in the VANETs. The idea of Trust computation has been a complementary approach to DRSC in the literature for efficient communication among vehicular nodes and the detection of reports from adversaries [5].
However, the existing trust algorithms are featured with pre- defined thresholds and complex iterations. These attributes can reduce the model performance in detecting malicious activities in the dynamic network and possible occurrence of latencies. Thus, inferences can be drawn that these models lack the flexibilities and functionalities in making sound predictions and decisions. VANETs based safety models require high reliability and low latency in their performance. Machine Learning/Deep Learning algorithms, remain suitable approach for analyzing and detecting security issues in VANETs. The effectiveness of ML/DL relies on the model ability to handle the dynamics of vehicular networks. We summarize the main contributions of this paper below:

- We provide a comparison of different ML/DL algorithms with different optimization techniques.
- We provide a model that can estimate the initial trust- worthiness on the information sent by the nodes in the absence of past experience about the nodes.

- We formulate trust evaluation by providing sound and intuitive trust attributes in V2V communication with the correlations of the Basic Safety Messages (BSMs).
- We provide a model with expert/prior information in terms of regularization implicitly. This will enhance pa- rameter defining in NN, avoidance of over-fitting and boost of model performance in case of data sparsity in a less densely populated vehicular network scenarios.
- We provide an efficient model with low detection latency in information capturing.

A. Generic Trust Framework

The concept of trust has received wider studies and applica- tions in different disciplines, like Philosophy, Sociology, and Politics as one of the major key factors in human decision making [5], [7]. Trust in the field of communication can be defined as the desired expectation from an agent to service rendered. This can be represented in different ways: for instance, a binary trust can be represented as ”1” or ”0”. A multilevel trust can be represented as level 1, level 2 ,..., level n , while a real value trust can be represented by values between [-1,1] and a probabilistic trust can have values between [0,1]. Trust management is categorized into three models, Entity Centric Trust (ECT), Data Centric Trust (DCT) and hybrid model. The paper lays emphasis on ECT and DCT models. In the ECT model, trust is being defined as an integration of multiple factors about the entity. In other words, trust is established on the nodes. This model of trust has been well adopted in trust computation in the literature. However, it has numerous drawbacks simply because of its time invariant nature. In this case, a valuable amount of time is taken for a receiving node to change the decision it must have taken about a given node. Furthermore, ECT involves rounds of complex iteration, which are likely to result in high detection latency of the system. This is not compatible with the dynamic nature of vehicular networks.

However, most of the emerging mobile networking tech- nologies are mainly data-centric in functionality and largely operated in a dynamic environment. Thus, in such a scenario, it is convenient to establish trust on the data rather than the reporting nodes. For instance, in VANET, the identity of nodes as a security measure in ECT has no contribution in the update of the events and status of the nodes in the network. However, DCT makes use of alert messages like the safety warnings, traffic information update, time freshness, and location relevance to provide a valuable information about the state of the vehicular network.

The above challenges of ECTs are addressed with the establishment of data centric attributes. In addition, ECT, relies heavily on the interactions of nodes in its decision making. A better appreciation of the malicious activities in the vehicular network can be felt with the numerous BSMs correlations integrated in DCT. These BSMs correlations are effectively used for trust modeling and the detection of attacks. The numerous attributes to measure trust are speed correlation with Emergency Electronic Break Light (EEBL), vehicular density with speed, distance of observing node to an event such as accident, and time of information report of incidence in the network.

In the ECT model, a decision is made based on the interaction between nodes. Decision making in this context involves the combination of direct trust, recommended trust, and previous experience of the receiving node about a re- porting node. The receiving node establishes some delays by waiting for the three message reports to be received before making a decision, thus subjecting the system to delay in decision making. In addition, in ECT management, nodes do not establish uniformity in similar observation of events.

II. BACKGROUND AND STATE OF THE ART

The challenges as a result of the dynamic, scalability and decentralized nature of vehicular networks have been a cause for concern in the security management of VANETs. The dynamic nature of VANETs, has introduced the scenario of uncertainty in the collection of evidence and trust evaluation. This section presents a brief review/insight on the existing trust computation models in the literature and also points out issues in addressing the security challenges in VANETs.

In respect to Machine Learning (ML), Raya et al [8] pro- posed the idea of DCT scheme in VANETs. Trust computation is evaluated using Bayesian and Dempster Shafer Theory (DST) techniques. In [9], a ML framework has been proposed for misbehavior classification using Weka[1]. In addition, au- thors in [10] used ensemble learning for misbehavior detection. However, the major challenge of Raya’s and Brijesh’s model is the performance efficiency in the training phase of their works. Authors in [11] proposed an adaptive detection model capable of preventing the effects of internal malicious attacks in vehicular networks. However, the model has low performance in event of high malicious attackers in the network. Related work in the literature, like Weighted Sum of received reports are used to establish DCT. The scheme proposed in [12], where reports from direct observer of an event assume the highest weight. The scheme only reduces the impact of oversampling due to multi-hop communications and works in the presence of honest majority. The loophole of this approach, is that it relies on the message contents to determine whether the node is a direct observer of the event or not. In [13], similarity measure is used in trust computation. In this regard, the similarity of the sender’s behavior for a

reported event is computed by an evaluator who sends back the same report to the sender in order to observe its reaction. This approach is susceptible to high overhead and prone to error as the sender gets closer to the events. In [14], [15], [16], sigmoid function was used in computing the result of non-linear function by considering the input vec- tors. In addition, in [17], back propagation of neural network is used to identify the spurious events and malicious nodes. The proposed model performs better than majority voting, simple weighted voting, and Bayesian approach. However, if the average reputation of the nodes is high the true positive rate decreases, coupled with the computational complexity involved in the model. The concept of fuzzy model is elegantly studied in the literature [18], [11], [19]. The model makes use of weighted sum of direct trust, indirect trust and Road Side [1]Weka is a suite of machine learning software written in Java, and developed at the University of Waikato, New Zealand.

Unit's (RSU) recommendation in identifying the state of events in a network [20]. It demonstrates high performance evaluation in detecting the malicious nodes but performs poorly, when the malicious activity in the network is high. In addition to [21] the membership is defined, indicating the magnitude of which node is taken to be trustworthy other than the binary set. The major challenge of this model from the point of view of [21] is that it requires the effort of domain expert in parameter tuning. Bayesian inference model has been well explored in the literature. The model adopts the probability and likelihood of honest behavior to establish trust. In [22], probability of honest and dishonest behaviors follow a Beta distribution and are used to establish trust. The proposed model is resilient to selective misbehavior attacks, since it does not consider the recommendation from neighboring nodes, it only relies on Direct Trust (DT). Although Bayesian Theorem provides a foundation for assessment of direct trust, it often includes belief discounting when there is a lack of evidence or the environment is noisy. In this paper, Bayesian Neural Network is proposed in comparison with Neural Network (NN). The hybrid model as investigated in [23], [24], is characterized for its ability to model uncertainty to check-mate the latent attributes of adversary nodes in the vehicular network and reduction of model complexity by performing regularization and cross validation independently. These attributes will effec-tively handle the detection of the hidden attributes of adversary nodes in the system which models in the literature have not effectively addressed.

B. Sybil Attack

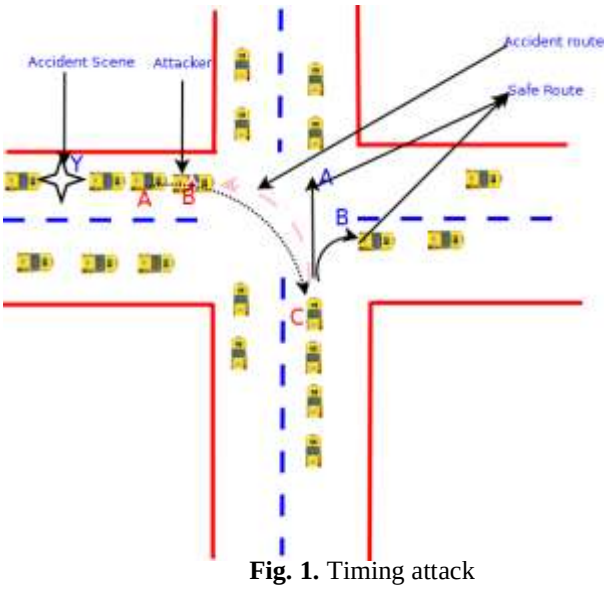

Fig. 1. Timing attack

$$\text{-} \quad \begin{matrix} 1 & if & t_g & tf < \varepsilon \\ 0 & | & otherwise \end{matrix} \qquad (2)$$

(2)

tively handle the detection of the hidden attributes of adversary nodes in the system which models in the literature have not effectively addressed.

III. SYSTEM ATTACK MODEL

This section demonstrates different attacks formulations.

A. Timing Attack

- Vehicle **B** is an attacker vehicle, which launches timing attack between vehicle **A** and vehicle **C**
- When **C** receives the broadcast message at the right time, it has basically two route options, **A** or **B** as directions to circumvent the accident at position **Y**
- However, if vehicle **C** receives a message with extra time slot added due to delay by timing attacker vehicle, vehicle **C** will eventually meet the accident scene.

According to Figure 1, vehicle **B** observes an accident event and initiates a broadcast to the neighboring vehicles.

Assuming that the time of event t_e and the sending time are the same. Thus, vehicle C, receives the message at expected time t_c

From the relationship between speed (v) and density (k) of vehicles, which are negatively correlated, it can be seen from equation 3, that increase in vehicular density results in the decrease in speed of vehicles. The reverse of this convention is assumed to be malicious. A clear illustration of the correlation of vehicular density with respect to speed is shown in Figure 2 and 3.

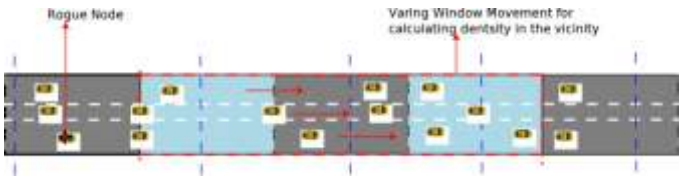

Fig. 2. Vehicular Density Estimation in VANET

$v(k) = v_f - \frac{k}{k_j} v_f$ (3)

Where v (k) = speed, v_f = free flow speed, k_j = jam density, k

$t_c = t_e +$ distance l_{Ct_c} c

Σ ,l_{Bt_e}

(1)

= density. In addition, an increase in the density of a vehicle, results in decrease in the speed until the density reaches the maximum, known as jam density. Effort should be made to

Where, t_c = expected time of message reception by the receiving node, l_{Ctc} = location of vehicle C at time t_c, while c, is the speed of light.
l_{Bte} = location of vehicle B at time t_e Thus:
The time verification T_v is true if $t_c - t_f < \varepsilon$ otherwise false. Where t_f is the received message by vehicle C, and ε represents a tolerable estimation error.
ensure that $v_s \pm v(k) \Delta$ where v_s is the speed of the sender. A negative value of v (k), implies that k exceeds maximum allowed density k_j which signifies a Sybil attack.

C. False Position Attack

A false position attack is changing the location of the vehicle by the attacker, and the vehicle is unable to detect

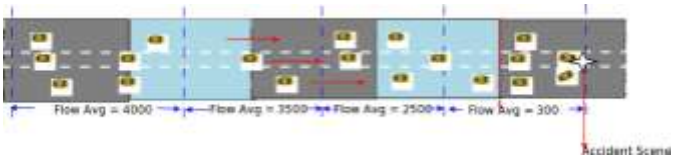

Fig. 3. Flow Variation in Accident Scene

this change and report it, as shown in Figure 4 and explained in more details as follows:

- Attacker Vehicle **B** discourages **A** from going further to broadcast warnings by pretending that it is closer to the incident of accident and in a better position **B'** to inform other vehicles.
- Vehicle **C** not being warned on time will likely meet the accident.

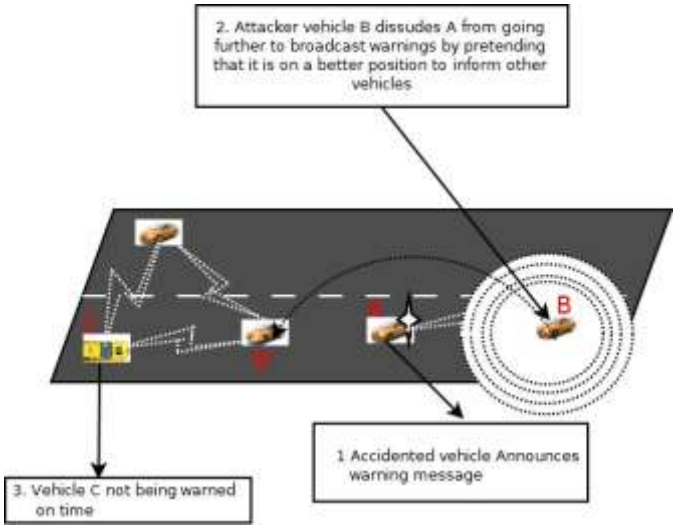

Fig. 4. False Position Attack

IV. METHODOLOGY

The paper proposes the Bayesian Neural Network (BNN) model framework for high performance prediction, classifica- tion accuracy and low detection latency, in trust computation in VANETs, when compared with NN, in the presence of uncertainty in the information. The inadequacy of NN, to capture the uncertainty in a network, can result in over-fitting
of the data collected from the nodes during the training phase, the hidden attributes and maintenance of a well performed generalization in trust computation in vehicular networks.
In addition, the Bayesian phase of the model will enhance the model selection by inferring the optimal number of com- ponents (feature extraction/feature selection). This is achieved by the model's calculation of the values of a given criterion of each of the models using Bayesian factors. The model selection attribute will extract the different features of different attackers, which can equally enhance the speedy detection of the variant of attacks in the vehicular networks. In line with [10], the feature extraction module combines the following attributes:

- VANETs model
- Attack model
- The VANETs application being attacked

The Figure 5 shows representation of work flow.

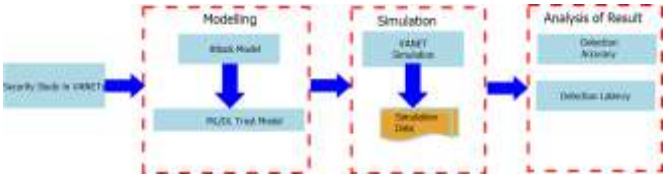

Fig. 5. Design Classification of Malicious and Honest Information

A. Mechanism of Operation of the BNN Model

The improvement of the NN model rests on its probability logic view [25], which has to do with the posing of NN and as a Bayesian process. The main goal of BNN is to uncover the full posterior distribution over the entire network weights. This idea of probabilistic estimation, in place of point estimation in traditional NN, makes BNN more robust and effective in handling the following issues:

1) Regularization process while fitting the data.
2) No need of separate cross validation of the information received by the nodes while doing model selection.
3) The probabilistic model of BNN handles uncertainty in a natural manner.
4) Bayesian defines an appropriate model space for the data, and as such implements the rule of inference numerically.
5) It enhances the automatic relevance determination (ARD) of the input parameters. To elaborate on the ARD; assuming that the weights w from the feature,

x_d have variance α_d^{-1} given that the p $w_{dj} | \alpha_d$ = $N(0, \alpha_d^{-1})$. When $\alpha_d \to \infty$ variance $\to 0$, $w \to 0$ and poor generalization of the model.

BNN maintains this high performance over NN in node's analysis, by providing a strong distribution and inclusion of uncertainty on the weights in the network. The uncertainty model enhances the practical framework in understanding the deep learning models. This also leverages the system to learn from a small amount of evidence [24] when Information sparsity is experienced in the vehicular network, capturing of designate irrelevant. On the other hand, when α_d ∞ finite variance weight can vary designate relevant. During this process, relevance inference of α is drawn from the data and while optimizing some α_d , it is possible that some will go to ∞, the model will discover some irrelevant inputs.

These attributes are not obtainable in the traditional NN setting and the parameters in NN require tuning by an expert Otherwise, it will lead to convergence at local minimum, and poor generalization of the model.

The idea of BNN framework is needed to overcome the challenges in NN. BNN incorporates the transformation of NN from point estimation to probabilistic estimation is achieved by first establishing series of functional transformation in different correlated layers. The mathematical representation is stated below: In this paper, Laplace's asymptotic approximation can be adopted to achieve the hyper-parameter selection.

B. Classification Criterion of the Model

This paper presents a detailed explanation of the mathe- matical representation of the detection and trust computation process while using BNN model in vehicular communication system. In this case, the model denotes x as a vector taken

$$y_k(x,\theta) = h\left(\sum_{j=1}^{H} w_{kj}^{(2)} h\left(\sum_{i=1}^{D} w_{ji}^{(1)} x_i + w_{j0}^{(1)}\right) + w_{k0}^{(2)}\right)$$

k_{th} neural network output. In other words, x is the piece of

from random variable D in the input layer, and y_k

$ji \quad j0 \quad +w^{(2)}$ (4)

is the $k0$

where y_k is taken to be the kth output of the neural network, x is the vector of the variable D for the input layer, while θ remains the combination of the adaptive weight parameters

evidence to be predicted. The variable *c* is the class of the

node with values 0 or 1. The value 0 and 1, respectively,
represent the malicious (mal) and honest (hon) information, sent by the nodes. Mathematically, $c \in \{mal,hon\} \equiv c \in \{0,1\}$
$w^{(1)}$
and $w^{(2)}$, and the bias $w^{(1)}$
and $w^{(2)}$, while H is the
considering a binary classification. The trust level correspond-
ji k j
j0 k0
ing to the class c, remains the posterior probability of c given
number of units in the hidden layer.
From the traditional approach, the variable θ from the training samples is estimated by possible minimization of the error function [26], [25]
the evidence $[\theta, \dot{X} = \dot{D}]$. This can be expressed using Bayes Theorem as follows:

$$p(c = C \mid \theta, \dot{X} = \dot{D}) =$$

$$\frac{1}{2} \quad \frac{N \quad N_o}{\alpha} \quad \frac{n}{W} \quad \{ \quad - \}$$

$$2 \qquad 2$$

$$2$$

$$p\ \theta \mid c = C, \dot{X} = \dot{D} \quad (c = C \mid \dot{X} = \dot{D})$$

$$E = E_D + E_\theta = \quad \sum \sum y_k (x ; \theta) \quad c_k$$
$$n=1 \ k=1$$
$$+ \quad \sum \theta_i \quad (5)$$
$$i=1$$
$$(\theta \mid \dot{X} = \dot{D})$$

where y_k denotes the kth neural network output with respect to x^n, of the nth training input data; c^n remains the nth target of the output training data, N is the corresponding input and output pairs in the target data set; N_o is denoted as the number of output variables;while W is the number of parameters in θ and α is the regularization parameter.The variable E_D and E_θ remain the error between the data and the approximation with respect to neural network and decay regularization.

To make the neural network assume the form of Bayesian frame work, the learning is to be interpreted from probabilistic angle [25], by considering the network output as the mean output which is conditional on the input [26], [25]. In addition, the prediction error should be interpreted probabilistically by adopting appropriate prediction error model like independent and identical, i.i.d Gaussian Probability distribution function PDF. [27].
The making of the neural network to assume a Bayesian
function (PDF) p (w | α, M), to give the posterior PDF as: form, leads to the update of the prior probability distribution
(8)
By application of total probability theorem, 8 can be ex- pressed as follows:
$p(c = C \mid \theta, \dot{X} = \dot{D}) =$
$P(\theta \mid c = C, \dot{X} = \dot{D}) p(c = C \mid \dot{X} = \dot{D})$

$\sum_{c\ (mal,hon)} [p(\theta\ \ c = C, \dot{X} = \dot{D}) p(c = C\ \ \dot{X} = \dot{D})]$ | |∈
(9)
For possible expression of mathematical simplicity, it is assumed that the individual reports remain independent [8]. From conditional probability of honest and malicious in- formation in vehicular networks the following mathematical expression is shown:
$p(mal \mid \dot{x}) + p(hon \mid \dot{x}) = 1$ (10) It can be deduced from equation 10, that $\dot{X}$ is malicious,

$p(\theta \mid D, \alpha, \beta, M) = \frac{p(D \mid \theta, \beta, M) p(\theta \mid \alpha, M)}{p(D \mid \alpha, \beta, M)}$ (6)

when $\dot{X} = 1$ $p(hon\ \dot{x})$. Threshold selection for the categorization of the information sent by the nodes into malicious and

Where M is the model, D is the Data and β and α are the hyper-parameters. Having done the necessary learning with the integration of Bayesian inference in NN, possible evaluation of the hyper-parameters is made. We assumed that the values of α and β , are unknown. Bayesian inference in this regard can be applied to make an adaptive selection of the hyper-parameters. The Baye's equation for this selection is represented below:
honest classes is adaptively done during Bayesian optimiza- tion of hyper-parameter, feature selection process and weight balancing of the nodes in Neural Network.
Without loss of generality, the model in this paper adopts the threshold of 0.5 as illustrated in Figure 6 for possible expression of the mathematics behind the classification process
of honest and malicious information. The, $\dot{X}$ is malicious iff
$p(mal \mid \dot{x}) > 0.5 \equiv 1 - p(hon \mid \dot{x})$.

$p(\alpha, \beta\ D, M) = \frac{p(D \mid \alpha, \beta, M) p(\alpha, \beta \mid M)}{p(D \mid M)}$
(7)
The posterior probability of equation 10 for malicious information is represented as follows:

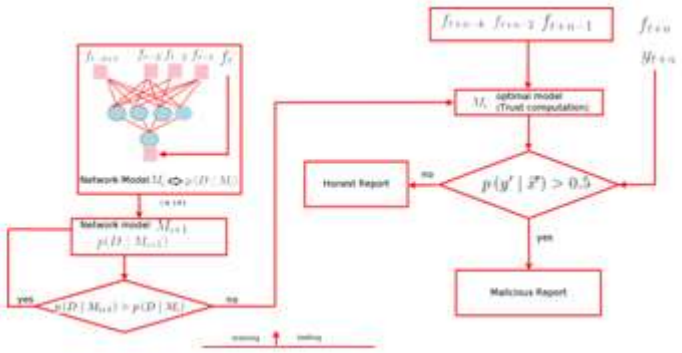

Fig. 6. Anomalies Detection chart

$$p(c = C \mid \theta, \dot{X} = \dot{D}) = \frac{P(\theta \mid c = C, \dot{X} = \dot{D})\, p(c = C \mid \dot{X} = \dot{D})}{\sum_{c \in (mal,hon)} [\, p(\theta \mid c = C, \dot{X} = \dot{D})\, p(c = C \mid \dot{X} = \dot{D})]}$$

$$> 0.5 \quad (11)$$

V. CONCLUSION AND FUTURE WORKS

This paper argues that ECT lacks the flexibility and effec- tiveness in detecting the malicious activities in the vehicular communication network. Thus DCT category is applied in the computation of trust in this paper. This paper further denotes that the existing algorithms on DCT in the literature are predefined/threshold based, and as such not capable enough to detect the dynamic behaviors of the adversaries in the communication systems. Consequently, the BNN trust model is proposed for the computation of the behaviors of the nodes in VANETs. The model is quite generic in nature and conceptually, goes beyond the existing trust models in the literature by including both perception and inference in it decision making. The improvement in the model performance as result of perception and inference of the hidden feature of malicious nodes is attributed to the introduction of uncertainty on the nodes in the network.

Our future work aims at implementing the proposed frame- work in Veins simulator and providing simulation experiments, and further do analysis and estimation of the nodes behaviour based on the information provided with the proposed BNN model.

REFERENCES

[1]. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," Journal of network and computer applications, vol. 37, pp. 380–392, 2014.

[2]. M. Chaqfeh, A. Lakas, and I. Jawhar, "A survey on data dissemination in vehicular ad hoc networks," Vehicular Communications, vol. 1, no. 4, pp. 214–225, 2014.

[3]. T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," Vehicular Communications, vol. 9, pp. 268–280, 2017.

[4]. R. Pal, A. Prakash, R. Tripathi, and D. Singh, "Analytical model for clustered vehicular ad hoc network analysis," ICT Express, 2018.

[5]. S. Ahmed, S. Al-Rubeaai, and K. Tepe, "Novel trust framework for ve- hicular networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9498–9511, 2017.

[6]. R. A. Shaikh and A. S. Alzahrani, "Trust management method for ve- hicular ad hoc networks," in International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer, 2013, pp. 801–815.

[7]. J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 562–583, 2011.

[8]. M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data- centric trust establishment in ephemeral ad hoc networks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008, pp. 1238–1246.

[9]. J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in vanet," in International Conference on Advances in Computing and Communications. Springer, 2011, pp. 644–653.

[10]. J. Grover, V. Laxmi, and M. S. Gaur, "Misbehavior detection based on ensemble learning in vanet," in International Conference on Advanced Computing, Networking and Security. Springer, 2011, pp. 602–611.
[11]. Y.-C. Wei and Y.-M. Chen, "Adaptive decision making for improving trust establishment in vanet," in Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific. IEEE, 2014, pp. 1–4.
[12]. Y. Yang, Q. Feng, Y. L. Sun, and Y. Dai, "Reptrap: a novel attack on feedback-based reputation systems," in Proceedings of the 4th interna- tional conference on Security and privacy in communication netowrks. ACM, 2008, p. 8.
[13]. H. Al Falasi, N. Mohamed, and H. El-Syed, "Similarity-based trust man- agement system: Data validation scheme," in International Conference on Hybrid Intelligent Systems. Springer, 2016, pp. 141–153.
[14]. B. Zong, F. Xu, J. Jiao, and J. Lv, "A broker-assisting trust and reputation system based on artificial neural network," in Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on. IEEE, 2009, pp. 4710–4715.
[15]. [15]J. Zhang, L. Huang, H. Xu, M. Xiao, and W. Guo, "An incremental bp neural network based spurious message filter for vanet," in Cyber- Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on. IEEE, 2012, pp. 360–367.
[16]. J. L ópez and S. Maag, "Towards a generic trust management framework using a machine-learning-based trust model," in Trust- com/BigDataSE/ISPA, 2015 IEEE, vol. 1. IEEE, 2015, pp. 1343–1348.
[17]. Y. L. Sun, Z. Han, W. Yu, and K. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings. IEEE, 2006, pp. 1–13.
[18]. A. Mudassir, S. Akhtar, H. Kamel, and N. Javaid, "A survey on fuzzy logic applications in wireless and mobile communication for lte networks," in Complex, Intelligent, and Software Intensive Systems (CISIS), 2016 10th International Conference on. IEEE, 2016, pp. 76– 82.
[19]. N. Griffiths, "A fuzzy approach to reasoning with trust, distrust and in- sufficient trust," in International Workshop on Cooperative Information Agents. Springer, 2006, pp. 360–374.
[20]. F. G. M ármol and G. M. Pérez, "Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934–941, 2012.
[21]. Y. Wang, "Trust-based service management for service-oriented mobile ad hoc networks and its application to service composition and task assignment with multi-objective optimization goals," Ph.D. dissertation, Virginia Tech, 2016.
[22]. X. Ma and X. Chen, "Delay and broadcast reception rates of highway safety applications in vehicular ad hoc networks," in 2007 Mobile networking for vehicular environments. IEEE, 2007, pp. 85–90.
[23]. Z. Ghahramani, "A history of bayesian neural networks," in NIPS Workshop on Bayesian Deep Learning, 2016.
[24]. Y. Gal, "Uncertainty in deep learning," University of Cambridge, 2016.
[25]. S. Arangio and J. Beck, "Bayesian neural networks for bridge integrity assessment," Structural Control and Health Monitoring, vol. 19, no. 1, pp. 3–21, 2012.
[26]. C. Bishop, C. M. Bishop et al., Neural networks for pattern recognition. Oxford university press, 1995.
[27]. E. T. Jaynes, Probability theory: the logic of science.Cambridge university press, 2003.