International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 2716–2725

Secure VANET Communication for Malicious Node Detection using a Classifier Model

[1]Gudivada Lokesh, [2]P Bhanu Prakash

[1,2]Assistant Professor

[1,2]Department of CSE

[1,2]Vemu Institute of Technology, Andhra Pradesh, India

[1]lokeshgvemu@gmail.com, [2]bhanuprakash.pakala13@gmail.com

Abstract

Vehicular ad-hoc networks (VANETs) are vulnerable to various attacks because of its dynamic in nature. The significance in the VANET is to estimate the trustworthiness of a vehicle for improving communication security. The several works have been done in the secure communication between the vehicular nodes. But accurate attack detection is still challenging to improve communication security in VANET. In order to improve secure communication in VANET with minimal time consumption, a Multi-Objective Reweighted Adaptive Boosting Classifier based Attack Detection technique is introduced. Reweighted Adaptive Boosting Classifier is an ensemble classifier which creates several weak learners. For classifying the vehicle nodes as normal or attack, the artificial neural network (ANN) is employed as a weak learner. Weak learner includes three layers namely input layer, hidden layer and output layer. Input layer obtains number of vehicle nodes. In hidden layer, multiple objective functions like trust, energy and cooperativeness of the vehicle nodes are computed. The Gaussian activation function is used at the output layer to classify the node as normal or attack based on the multiple objective functions of the vehicle nodes. At last, the approach combines the weak classifier output and offers strong classification results with lesser error rate. Therefore, the attack nodes are detected with minimal energy consumption. Simulation is conducted with metrics namely detection rate (DR), false positive rate (FPR) and detection time (DT) with number of vehicular nodes.

Keywords: *VANET, secure communication, attack detection, Multi-Objective reweighted Adaptive Boosting Classifier, ANN, Gaussian activation function*

1. Introduction

VANETs are the assuring network scenario where one vehicle nodes communicate to other vehicles. VANET is an infrastructure less network since it does not have any fixed access point. The random mobility of vehicle nodes degrades the vehicle communications thus impacting network security. In VANET, the malicious node can alter the communication among the vehicles. Therefore, an efficient attack detection technique is required in the VANET for improving the communication security.

The major problems are identified from the above-said existing works such as lack of improving the DR, higher FPR, more DT, lack of improving the security and failure to consider the energy and so on. In order to overcome such kind of issues, an efficient technique called MORABC-AD is developed in VANET.

The major contributions of MORABC-AD technique are summarized as follows,

ISSN: 2233-7857 IJFGCN

- The MORABC-AD is presented to improve the security in data communication by detecting the attack in VANET. This contribution is achieved using Multi-Objective Reweighted Adaptive Boosting Classifier. Multi-Objective Reweighted Adaptive Boosting is an ensemble classifier which uses the ANN as a weak learner. The ANN takes the inputs as the number of vehicle nodes in the input layer. The multiple objective functions (i.e. trust, energy, cooperativeness) of the vehicle node are calculated at the hidden layer. This assists to increase the DR.

- To minimize the detection time, the ANN uses the Gaussian activation function at the output layer. The Gaussian activation function analyses the node with their multiple objective functions and classifies the node as normal or attack.

- To enhance the DR and lessen the FPR, the weak learners are reweighted depending on their training error. MORABC discovers the weak learner with lesser error using argument of minimum function. The nodes with higher residual energy, higher trust value and better cooperativeness are classified as a normal node. Otherwise the nodes are said to an attack node.

`

2. Related works

In [11], a Trust-aware Collaborative Learning Automata based Intrusion Detection System was introduced. The system increases the detection ratio and minimizes the false alarm rate but it failed to consider the node behaviors like energy and cooperative communication. To detect the intrusions with respect to trust and cooperativeness, a host-based intrusion detection system was designed in [12]. The system did not use any machine learning classifier for effectively improving the DR with minimum time.

In [13], a Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) was introduced to classify the Denial of Service (DoS) and black hole attacks. The analysis achieves a minimum false alarms rate and a higher DR. But it failed to minimize the DT.

To improve the security of network, a deep neural network (DNN) was designed in [14]. However, the FPR was higher. In [15], a Support Vector Machine (SVM) and Dempster-Shafer theory were introduced for misbehavior detection. But, it does not lessen the time taken for detecting the misbehavior vehicle in the network.

A Dedicated Short-Range Communication (DSRC) system was presented in [16] to discover the malicious nodes with the minimum false positive rate. The system failed to estimate the behavior of the node for achieving a better DR.

The issues of conventional methods are overcome by introducing a MORABC-AD technique. The processes of MORABC-AD technique are explained in the next section.

3.Multi-Objective Reweighted Adaptive Boosting Classifier based Attack Detection in VANET

ISSN: 2233-7857 IJFGCN

In VANET, numbers of nodes (i.e. vehicles) are distributed randomly without any predefined infrastructure. VANET is susceptible to varieties of attacks which degrades the entire network performances as well as secure data communication. The ability to use an attack detection technique is an additional concern for improving security in communication. Based on this motivation, the MORABC-AD technique is introduced. By applying MORABC-AD technique, the vehicles nodes are classified into normal or attack.

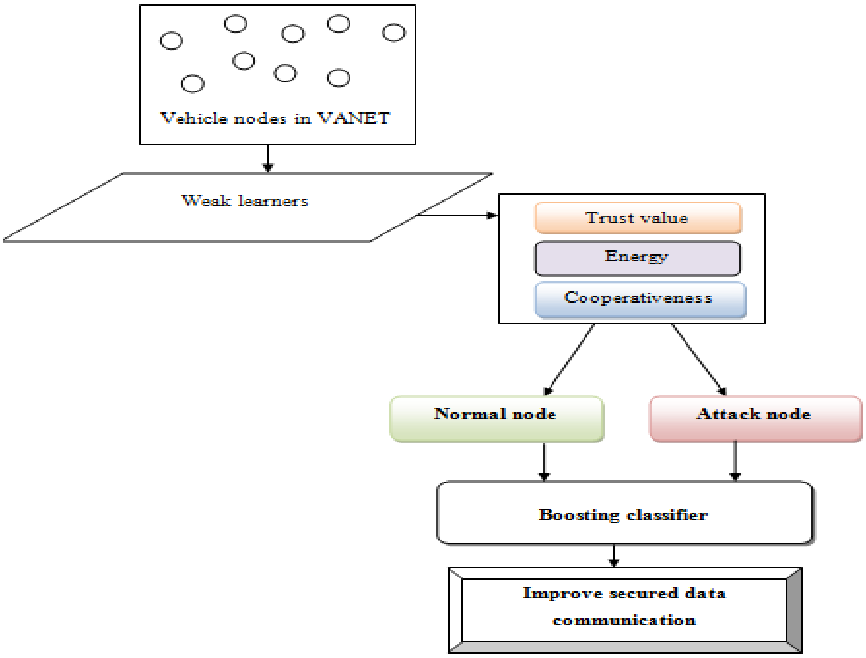

Figure 1 architecture diagram of proposed MORABC-AD technique

The architecture diagram of MORABC-AD technique is shown in figure 1 to enhance the attack DR with minimum time. In VANET, numbers of vehicle nodes are distributed in a random manner. The reweight adaptive boosting classifier categorizes the vehicle nodes into normal or attack based on the nodes behaviors like trust value, energy and cooperativeness with high accuracy. Based on the above-said behavior of the vehicle nodes, the classification is done using ensemble classifier.

The normal nodes for increasing security in data communication. In MORABC-AD technique, the ANN is used as a weak learner for classifying the nodes as a normal node or abnormal node.

The process flow of reweighting adaptive boosting classifier for identifying the malicious node in VANET. The reweight adaptive boosting classifier uses a training set $\{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$ where 'x' denotes a number of vehicle nodes$vn_1, vn_2, vn_3, \ldots\ldots vn_n$, '$y$' denotes a classification output$\{+1, -1\}$. ANN is used as a weak leaner of ensemble classifier. For enhancing the classification performance with minimal error rate, the strong learner combines weak classifier results to form the strong classifier. ANN includes the collection of units known as artificial neurons. An artificial neuron network includes three layers such as input, hidden and output layer where connection transmits an input from one layer to another which is shown in figure 3.

ISSN: 2233-7857 IJFGCN

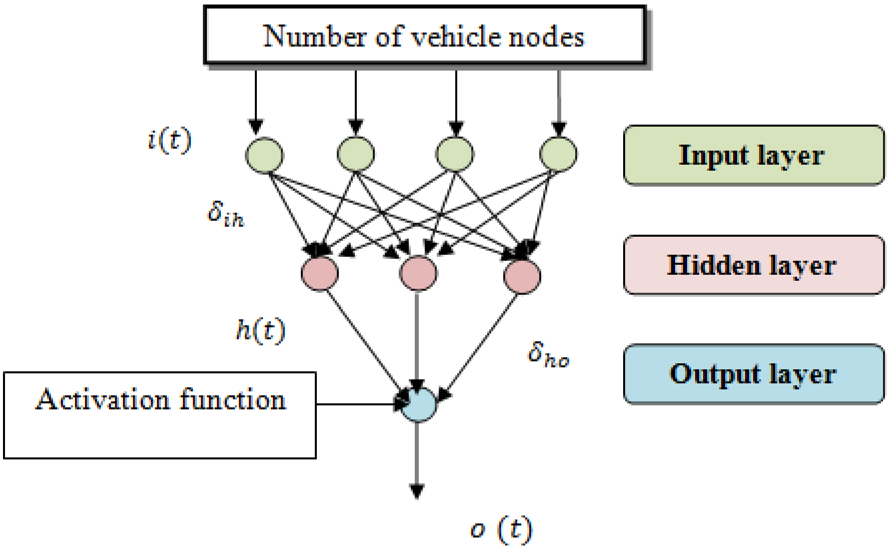

Figure 3 structure of ANN

The structure of the ANN with three different layers. The input layer receives number of vehicles nodes at a time 't' is represented as '$i(t)$'. The nodes behaviors are computed in the hidden layer. The hidden layer output and output layer are represented as '$h(t)$ and '$o(t)$'. Through dynamic weights δ_{ih} and δ_{ho}, the input, hidden and output layers are interconnected. In the hidden layer, the nodes behaviors such as trust, energy and cooperativeness are computed.

Let us consider the number of vehicle nodes $vn_1, vn_2, vn_3, \dots . . vn_n$. The trust values of the nodes are computed as the difference between the numbers of data packets dropped and numbers of data packets forwarded as well as received by the vehicle nodes. The trust value of the each vehicle node is calculated using the below equation,

$$T_r = \frac{dp_F - dp_D}{dp_R} \quad (1)$$

From (1) T_r represents the trust of the nodes, dp_F denotes a data packet forward rate, dp_D denotes a data packet dropped rate, dp_R denotes a data packet received by the node.

4.Energy

The node energy is computed after calculating the nodes trust value. Based on the product of power and time, the energy of vehicle node is calculated. The energy is calculated as follows,

$$E = power * time \quad (2)$$

From (2), E represents the energy of the nodes, power is measured in watts and time is measured in seconds (Sec). The energy of each node is measured in terms of a joule (J). After that, the energy of the each sensor nodes gets degraded and the remaining energy (i.e. residual energy) of the nodes are calculated as follows,

$$R_E = T_E - C_E \quad (3)$$

In (3), $R_E$represents the residual energy, T_E denotes a total energy, C_E is the consumed energy of the vehicle nodes. The residual energy of the sensor nodes are used

ISSN: 2233-7857 IJFGCN

to determine which nodes utilize the more energy.

5.Cooperativeness of the node

The cooperativeness is the major behavior of the nodes for identifying the attack nodes in VANET. The attack nodes have known the information about the network and they do not cooperate with the other nodes for better communication. Therefore, the cooperativeness of the nodes is also used to guarantee the links between the vehicle nodes over the time instant for preserving the connections between the nodes. The links between the nodes are identified through the two control message distributions. The control messages are route request (RREQ) and route reply (RREP) are distributed between the two vehicle nodes. The vehicle node vn_1 send a request message to other neighboring node for establishing the links.

$$vn_i \overset{RREQ}{\Rightarrow} vn_j \quad (4)$$

In (4), the vehicle node vn_i sends route request $(RREQ)$ to vn_j in the network. The node vn_j sends the reply message $RREP$ back to the node vn_i .

$$vn_i \overset{RREP}{\Leftarrow} vn_j \quad (5)$$

In (5), the vehicle nodes vn_j sends a reply message $RREP$ to the vehicle node vn_i, then the node vn_i is connected to vn_j at the time instant. If the vehicle node vn_i did not receives the reply message from the vn_j, these two nodes are not connected at the particular time 't'. Then the node vn_i detects the misbehaving nodes in network. The node cooperativeness is determined based on the link estimation. The hidden layer output is formalized as follows,

$$h(t) = \delta_{ih} * i\ (t) \qquad (6)$$

In (6), $h(t)$ signifies the hidden layer output, δ_{ih} indicates a weight between the input and hidden layer, $i\ (t)$ indicates an input. Finally, the output layer classifies the vehicle node as normal or abnormal using an activation function. Therefore, the weak learner output is formalized as below,

$$o(t) = \sigma_f * \{\delta_{ho} * h(t)\} \quad (7)$$

In (7),$o\ (t)$ denotes an output of an artificial neural classifier, σ_f denotes an activation function, δ_{ho} represents a weight between the hidden and an output layer. The weak learner uses the Gaussian activation function.

$$\gamma_f = \frac{1}{\sqrt{2\pi\sigma}}\ exp\ (\frac{-(x-\mu)^2}{2\sigma^2})\ (8)$$

From (8),γ_f denotes a Gaussian activation function to provides the two binary results such as '0' and '1'. If the activation function provides the results as '0', then the nodes is said to an abnormal node. If the activation function provides '1', then the vehicle nodes are classified as a normal node. The attack nodes are correctly identified in the output layer based on the classification results.

ISSN: 2233-7857 IJFGCN

A weak learner causes the error during the classification. For enhancing the performance of classification with minimal error rate, the MORABC classifier combines weak learner's output to create the strong classifier. To acquire strong classification results, the weak classifiers are combined as below,

$$y_i = \sum_{i=1}^{n} b_i(x) \quad (9)$$

In (9), y_i indicates the output of strong classifier, $b_i(x)$ indicates the output of weak learners. Then, the similar weight is assigned to each weak learner.

$$\beta_t \rightarrow \sum_{i=1}^{n} b_i(x) \quad (10)$$

In (10), β_t denotes a weight assigned to each weak learners $b_i(x)$. The training error of every weak learner is calculated after assigning the similar weights. The error is measured as squared difference between actual and predicted results that is formalized as below,

$$t_E = (o_i - b_i(x))^2 \quad (11)$$

In (11), t_E denotes the training error of weak learner, o_i indicates an actual output of weak learner and $b_i(x)$ indicates the predicted output of weak learner. Based on the error rate, the weak learners are reweighted. The reweighting equation is represented as below,

$$\beta_t' = \frac{\beta_t * \exp(-\gamma_t y_i b_i(x))}{N_t} \quad (12)$$

In (12), β_t' indicates a reweight of weak learner, β_t symbolizes the initial weight of weak learner, γ_t denotes a adjustment coefficient to attain strong classification results. y_i denotes a true class and $b_i(x)$ represents the predicted class, N_t represents the normalization constant. If the weight is enhanced, the weak learner wrongly classified vehicle nodes as normal or attack. The weight is reduced, then the weak learner correctly classified vehicle nodes as normal or attack. The equation (12) is also expressed as ,

$$\beta_t' = \frac{1}{N_t} \beta_t * \begin{cases} \exp(-\gamma_t) & if \quad b_i(x) = y_i \\ \exp(\gamma_t) & if \quad b_i(x) \neq y_i \end{cases} \quad (13)$$

In (13), γ_t denotes an adjustment coefficient which is expressed as follows,

$$\gamma_t = 0.5 \, log \left(\frac{1 - t_E}{t_E} \right) \quad (14)$$

In (14), t_E indicates a training error of weak learner, then weak learner with minimal error is chosen as better results.

$$\arg\min t_E \, (b_i(x)) \quad (15)$$

From (15), $arg\ min$ denotes an argument minimum of a function and 't_E' denotes an error of the weak learner $b_i(x)$. Then, the best leaner is trained to get the final output as follows,

$$S(x) = sign\left(\sum_{i=1}^{n} \beta_t * b_i(x)\right) \quad (16)$$

From (16), $S(x)$ denotes an output of a strong classifier, $sign$ indicates the positive and negative results of the final output classifier.

ISSN: 2233-7857 IJFGCN

The final strong classifier output $\beta_t * \; b_i(x) = +1$ represents the nodes are correctly classified as normal nodes or attack if the true class (y_i) equals to the predicted class $b_i(x)$. Whereas -1 denotes the nodes are incorrectly classified as normal or attack i.e. true class (y_i) is not equals to the predicted class $b_i(x)$. The above results show that the normal or attack nodes are correctly detected to improve the secure communication. After finding the attack nodes, the communication is performed through the normal node and attained the high security in data communication.

Input: Number of vehicle nodes $vn_1, vn_2, vn_3, \dots . vn_n$

Output: Increase attack detection rate

Begin

1. Construct a number of weak learners i.e. ANN
2. Given the vehicle nodes vn_i into the input layer
3. Transform input to the hidden layer
4. **For** each vn_i
5. Compute trust value, residual energy and cooperativeness
6. **If** the activation function $(\gamma_f = 1)$ **then**
7. Nodes are classified as normal
8. **else**
9. Nodes are classified as an attack
10. **End if**
11. **End for**
12. Combine all weak learners output $\sum_{i=1}^{n} b_i(x)$
13. Initialize similar weights $\beta_t \rightarrow b_i(x)$
14. Calculate the training error $t_E = (y_i - b_i(x))^2$
15. Reweight the weak learner $\beta_t{}'$
16. Find weak learner $b_i(x)$ that minimizes training error t_E
17. The output of final strong classifier $S(x) = sign\,(\sum_{i=1}^{n} \beta_t * \; b_i(x))$

End

Algorithm 1 Multi-Objective reweighted Adaptive Boosting Classifier based Attack Detection

Above Algorithm describes the classification of normal vehicle node or attack node in VANET. Initially, the ensemble classifier builds the number of weak learners. ANN is employed as a weak learner to classify the nodes in VANET. The input i.e. vehicle nodes are taken as input. In the hidden layer, the nodes residual energy, trust value, cooperativeness is computed. The nodes with higher trust and maximum residual energy and better cooperativeness are classified as a normal node using the Gaussian activation function. Otherwise, the nodes are said to be an attack node. The weak learners' results are summed to create a strong result. The similar weights are initialized to all the weak learners. Then, the training error is calculated for each weak learner output. The nodes are reweighted depending on their error value. By finding the weak learner with lesser training error, the strong classification results are obtained. The data communication is performed through the normal node for attaining high security.

ISSN: 2233-7857 IJFGCN

The above algorithmic process is applied to improve the performance of MORABC-AD technique compared with the conventional methods.

6. Simulation Settings

An efficient MORABC-AD technique and existing methods namely GDVAN [1] and multi-layered game theory based intrusion detection framework [2] is implemented in NS2.34 network simulator. For detecting the attack or normal node, Totally 500 vehicle nodes are deployed in a square area of A^2(1000 m * 1000 m) to improve the security of data communication in VANET. The two ray ground model is used as radio propagation in the simulation. The vehicle nodes speed is set as 10-30m/sec and the simulation time is 240 sec. The various simulation parameters and its values are listed in table1.

Table 1 Simulation parameters

Simulation Parameters	Values
Simulator	NS2.34
Network area	1000 m * 1000 m
Number of vehicle nodes	50,100,150,200,250,300,350,400,450,500
Radio Propagation Model	Two Ray Ground
Vehicle nodes speed	10 – 30 m/s
Simulation time	240sec
Channel bandwidth	6Mbps
Number of runs	10

The simulation is performed based on the number of vehicle nodes with various parameters such as DR, FPR and DT using the above-said simulation settings. The results of the various parameters using three different methods are discussed in the next section.

7. Results and Discussions

The simulation results of proposed MORABC-AD technique and existing techniques namely GDVAN [1] and multi-layered game theory based intrusion detection framework [2] are described with various parameters such as DR, FPR and DT. The performance of proposed MORABC-AD technique is compared with the existing methods using table and graphical results.

8. Conclusion

An efficient technique called MORABC-AD is developed to improve security during the data communication between the vehicles in VANET. Initially, the MORABC constructs a number of weak learners to classify the vehicle node as normal or attack based on the multiple objective functions. The MORABC uses the ANN as weak learners for performing the classification which uses the three layers. The Gaussian activation function is used at the output layer for classifying the node resulting in minimizes the detection time. The results of weak learner's are combined into a strong and assign the weight value. After that, the weak learners are reweighted based on the error value.

ISSN: 2233-7857 IJFGCN

9. References

[1] Mohamed Nidhal Mejri and Jalel Ben-Othman, “GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs”, IEEE Transaction on Mobile Computing, Volume 16, Issue 3, March 2017, Pages 759 – 771.

[2] Basant Subba, Santosh Biswas, Sushanta Karmakar, “A game theory based multilayered intrusion detection framework for VANET”, Future Generation Computer Systems, Elsevier, Volume 82, May 2018, Pages 12-28

[3] Uzma Khana, Shikha Agrawala, Sanjay Silakaria, “Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks”, Procedia Computer Science, Elsevier, Volume 46, 2015 , Pages 965 – 972

[4] Sheeraz Ahmed , Mujeeb Ur Rehman, Atif Ishtiaq, Sarmadullah Khan, Armughan Ali, and Shabana Begum, “VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead”, Journal of Sensors, Hindawi, 2018, 16 July 2018, Pages 1-17

[5] Wenjia Li and Houbing Song, “ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks”, IEEE Transactions on Intelligent Transportation Systems, Volume 17, Issue 4, 2016, Pages 960 - 969

[6] Karan Verma and Halabi Hasbullah, “Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET”, Security and Communication Networks, Volume 8, 2015, Pages 864–878

[7] Raenu Kolandaisamy, Rafidah Md Noor, Ismail Ahmedy, Iftikhar Ahmad ,Muhammad Reza Z’aba, Muhammad Imran and Mohammed Alnuem, “A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks”, Wireless Communications and Mobile Computing, Hindawi, Volume 2018, May 2018, 13 page

[8] Jyoti Grover , Vijay Laxmi , Manoj Singh Gaur, “Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks”, CSI Transactions on ICT, Springer, Volume 1, Issue 3, September 2013, Pages 261–279

[9] Jay Rupareliya, Sunil Vithlanib, Chirag Gohel, “Securing VANET by preventing attacker node using Watchdog and Bayesian Network Theory”, Procedia Computer Science, Elsevier, Volume 79, 2016, Pages 649 – 656

[10] Hichem Sedjelmaci and Sidi Mohammed Senouci, “An accurate and efficient collaborative intrusion detection framework to secure vehicular networks”, Computers & Electrical Engineering, Elsevier, Volume 43, April 2015, Pages 33-47

[11] Neeraj Kumar and Naveen Chilamkurti, “Collaborative trust-aware intelligent intrusion detection in VANETs”, Computers & Electrical Engineering, Elsevier, Volume 40, Issue 6, August 2014, Pages 1981-1996

[12] Kamran Zaidi, Milos B. Milojevic, Veselin Rakocevic, Arumugam Nallanathan, Muttukrishnan Rajarajan, “Host-based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection”, IEEE Transactions on Vehicular Technology,

ISSN: 2233-7857 IJFGCN

Volume 65, Issue 8, August 2016, Pages 6703 – 6714

[13] Khattab M.Ali Alheeti, Anna Gruebler, Klaus McDonald-Maier, "Using discriminant analysis to detect intrusions in external communication for self-driving vehicles", Digital Communications and Networks, Elsevier, Volume 3, Issue 3, August 2017, Pages 180-187

[14] Min-Joo Kang and Je-Won Kang, "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security", PLoS ONE, Volume 11, Issue 6, 2016, Pages 1-17

[15] Chunhua Zhang , Kangqiang Chen , Xin Zeng , Xiaoping Xue, "Misbehavior Detection based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs", IEEE Access , Volume 6, Pages 59860 – 59870

[16] Saneeha Ahmed , Sarab Al-Rubeaai , Kemal Tepe, "Novel Trust Framework for Vehicular Networks", IEEE Transactions on Vehicular Technology, Volume 66, Issue 10, 2017, Pages 9498 – 9511

[17] Celestine Iwendi , Mueen Uddin , James A. Ansere , P. Nkurunziza , J. H. Anajemba, Ali Kashif Bashir, "On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique", IEEE Access, Volume 6 , August 2018, Pages 47258 – 47267

[18] Chundong Wang , Zhentang Zhao , Liangyi Gong , Likun Zhu , Zheli Liu , Xiaochun Cheng, "A Distributed Anomaly Detection System for In-Vehicle Network Using HTM", IEEE Access, Volume 6, Pages 9091 – 9098

[19] Avleen Kaur Malhi and Shalini Batra, "Genetic-based framework for prevention of masquerade and DDoS attacks in vehicular ad-hoc networks", Security and Communication Networks, Volume 9, 2016, Pages 2612–2626

[20] Ameneh Daeinabi, Akbar Ghaffarpour Rahbar, "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks", Multimedia Tools and Applications, Springer, Volume 66, Issue 2, September 2013, Pages 325–338

ISSN: 2233-7857 IJFGCN