Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume12, Issue 5, July 2021: 3454-3468

Research Article

Sybil Misbehavior Detection in Software Defined VANETs using Received Signal Strength

[1]Rajendra Prasad Nayak, [2]Srinivas Sethi, [3]Sourav Kumar Bhoi, [4]Kshira Sagar Sahoo, [5]Mehedi Masud, [6]Mohammad Baz

Abstract

Software-defined Vehicular ad hoc Networks (SDVN) are the new research area where vehicular networks use the SDN technology for efficient network management. In SDN the network is divided into control plane and data plane by which the load of the network is efficiently managed. The control plane is responsible for building the rules and the data plane is responsible for transferring data between the devices or nodes. As important information such as safety-related, and non-safety related are exchanged between the vehicles, the nodes in the network should be legitimate. SDVN is mostly affected by many attackers in the network which disrupts the whole performance. One such most dangerous attack is Sybil attack where the attacker creates fake identities in the network to take control of the network. This attack should be detected well else the network performance decreases. In this paper, a Sybil misbehavior detection approach is proposed for SDVN using the Received Signal Strength (RSS) of a vehicle. The RSS values are computed by On Board Unit (OBU) when the beacons are regularly received from the neighboring vehicles. Then the vehicles with the same RSS values are grouped to check the nodes as Sybil nodes by finding the distances of the neighbor vehicles. The simulation is performed using OMNeT++ simulator and SUMO road traffic simulator. The method is compared with competing schemes. From the results, it is observed that the proposed approach performs better in terms of detection accuracy, false-positive rate, false-negative rate, and detection time.

Keywords: VANETs, SDVN, Sybil Attack, Misbehavior Detection, RSS

1. INTRODUCTION

Vehicular networks (VNs) are most advanced networks providing many safeties and non-safety applications to the users [1-3]. Safety applications includes accident alarming systems, collision detection, parking solutions, traffic detection, etc. Non safety applications include media

[1] Department of Computer Science and Engineering,Government College of Engineering, Kalahandi, BPUT University, India
[2]Department of Computer Science Engineering and Applications, IGIT Sarang (Govt.), BPUT University, India
[3]Department of Computer Science and Engineering, PMEC Berhampur (Govt.), BPUT University, India
[4]Department of Computer Science and Engineering, SRM University, Amaravati, AP, India
[5] Department of Computer Science, College of Computer and Information Technology, Taif University, PO Box. 11099, Taif 21994, Saudi Arabia
[6] Department of Computer Engineering, College of Computer and Information Technology, Taif University, PO Box. 11099, Taif 21994, Saudi Arabia
[1]rajendra.cet07@gmail.com,[2]srinivas_sethi@igitsarang.ac.in, [3]souravbhoi@gmail.com, [4]kshirasagar12@gmail.com, mmasud@tu.edu.sa, mo.baz@tu.edu.sa

uploading and downloading data, file transfer, gaming, internet access, etc. These communications are possible between the vehicles using V2V and V2I communications. V2V means vehicle to vehicle communication and V2I means vehicle to infrastructure communication, where infrastructure means roadside units (RSUs). VNs mainly uses standards for communication such as DSRC and WAVE [1-3]. DSRC means Dedicated Short Range Communications. WAVE means Wireless Access to Vehicular Environment. However, nowadays VNs mainly uses the 3G/4G/LTE, WiMax, etc. communications for better connectivity.

As VNs exchange valuable information between the vehicles the data transfer should be between the legitimate vehicles. Therefore, security is a major concern in VNs [4-6]. Many types are attacks are performed by the attackers to control the whole network for their use. This degrades the performance of the network where the legitimate vehicles are compromised or attacked by other malicious vehicles. One such most dangerous attack is Sybil attack where the attacker creates fake identities in the network to create the control over the network and performs negative actions for example packet dropping, jamming, routing attack, denial of service, data modification, etc. In this work, we have proposed a Sybil misbehavior detection approach to detect the Sybil nodes. For efficient management of the network and providing good security regarding the Sybil attack detection we have used SDN based technology [7-9]. SDN offers a greater potential for providing a secure and flexible network [31-33]. The basic SDN architecture is shown in Fig. 1 as follows. There are basically three layers such as Application layer, Control layer, and Data layer. The application layer provides safety and non-safety applications. In this work our main application is misbehavior detection of Sybil's attacker. The Control layer consists of a SDN controller which controls the whole system by designing the rules for each device connected to the network. The base layer is the Data layer where the data are exchanged between the nodes in the VNs. The application layer is connected to the control layer using the APIs (Application Peripheral Interfaces) and the control layer is connected to the data layer using the interface as shown in Fig. 1. This technology will better be suited to our environment for providing misbehavior detection.

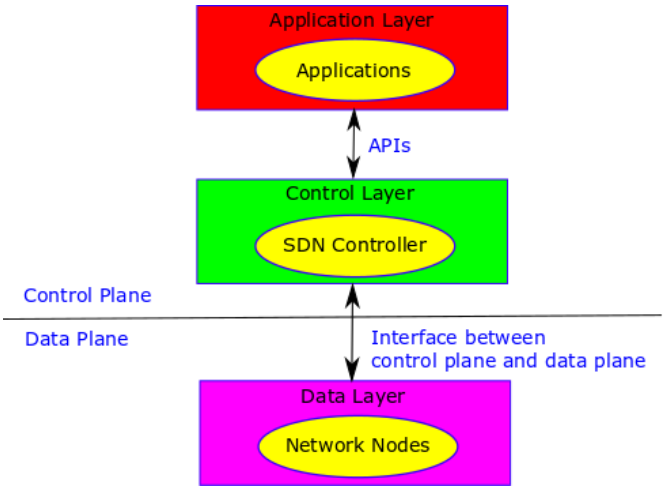

Fig. 1: SDN Architecture

In this work the major contributions are stated as follows: -

1. In this paper, a Sybil misbehavior detection approach is proposed for SDVN using the RSS value of a vehicle.
2. The RSS values are computed by the OBU when the beacons are regularly received from the neighboring vehicles. Then the vehicles with same RSS values are grouped. To check the nodes as Sybil nodes the distances of the neighbor vehicles are calculated using the RSS values.
3. The simulation is performed using OMNeT++ simulator and SUMO road traffic simulator. The method is compared with Grover et al. [10] and Grover et al. [11].
4. From results it is observed that proposed approach performs better in terms of detection accuracy, false positive rate, false negative rate, and detection time.

The rest the work is organized as follows. Section 2 presents the related works in Sybil misbehavior detection. Section 3 presents the network model, misbehavior model and proposed approach. Section 4 presents the simulations and results. Section 5 presents the conclusion and future scope of the work.

2. RELATED WORKS

Many research works have been done to detect the Sybil attack in VNs [10-29]. Grover et al. [10] proposed a RSS based sybil attack detection for VANETs. In this method, the RSS of the vehicles are collected by the RSUs and the vehicles with same RSS values are stored in a group and the vehicles with different RSS values are stored in another group. This method detects the sybil attackers well. However, this method totally dependent on the deployment of RSU, means if the number of RSU increases the detection accuracy also increases. This is a limitation of this scheme. Grover et al. [11] proposed another scheme where the neighboring vehicles are used to identify the sybil attackers. In this method if common neighbors are there for a particular amount of time with all the neighbors, then the group of nodes are called as Sybil nodes. However, if the sybil node generates fake identities after every regular interval then it will be a problem to detect the sybil attackers. Grover et al. [12] proposed another mechanism where they consider distance, angle, and RSS to find the actual sybil attacker. The parameters are calculated using the RSU. So, this method also depends on the RSU and if there is sparse network with less RSU then it may affect the process. Grover et al. [13] also finds another approach such as multivariate verification of sybil attack detection using the movement patterns of the nodes. However, these nodes also depend on the RSUs. Shrestha et al. [21] given a lightweight solution for detection of sybil nodes in vehicular networks. Many such research works are presented in [10-29], where the researchers use cryptographic solutions, trust solutions, machine learning solutions, etc. The researcher provided solutions for the malware identifications and two factor authentication [35-

38] for providing the security. In [39- 41] authors presented deep reinforcement methods and syn flood attack detections and how they affect the performance.

From the above study it is found that very less work has been done in software defined VANETs, where the application is misbehavior detection, and the whole rules are designed by the SDN controller. The data transfer is also managed well by the SDN controller at the data layer. So, it will be a new direction in detecting the Sybil attack using the RSS in SDVN.

3. PROPOSED SYBIL MISBEHAVIOR DETECTION APPROACH

In this section, we have mainly discussed about the network model and assumptions, sybil misbehavior model, and proposed misbehavior detection approach.

4.1. Network Model

This section describes about the network model and the communication between the nodes. The SDVN network is presented in Fig. 2 as follows. The network mainly consists of three layers such as Application layer, Control layer, and Data layer. The application layer provides misbehavior detection of Sybil attacker. The Control layer consists of a SDN controller (SDNC) which controls the whole system by designing the rules for each device connected to the network. The base layer is the Data layer where the data are exchanged between the nodes in the VNs. The application layer is connected to the control layer using the APIs and the control layer is connected to the data layer using the interface. The vehicles communicate using V2V communication. The vehicle communicates with the RSU using V2I and I2V communication. The RSU communicates with the base station (BS) using I2BS and BS2I communication. The BS communicates with the SDN using SDNC2BS and BS2SDNC communication.

The model assumptions are stated as follows. The vehicle consists of a OBU unit which is responsible for transmission/reception, computation, and storage. It has a GPS by which a vehicle can locate itself. The vehicle in the network sends beacon message at a regular interval of time. This beacon message consists of identity ID, current position (x_n,y_n), speed sp, and direction dir. Each vehicle maintains a neighbor table where they maintain the parameters of the beacons received from the neighboring vehicles. These are updated after each beacon is received.

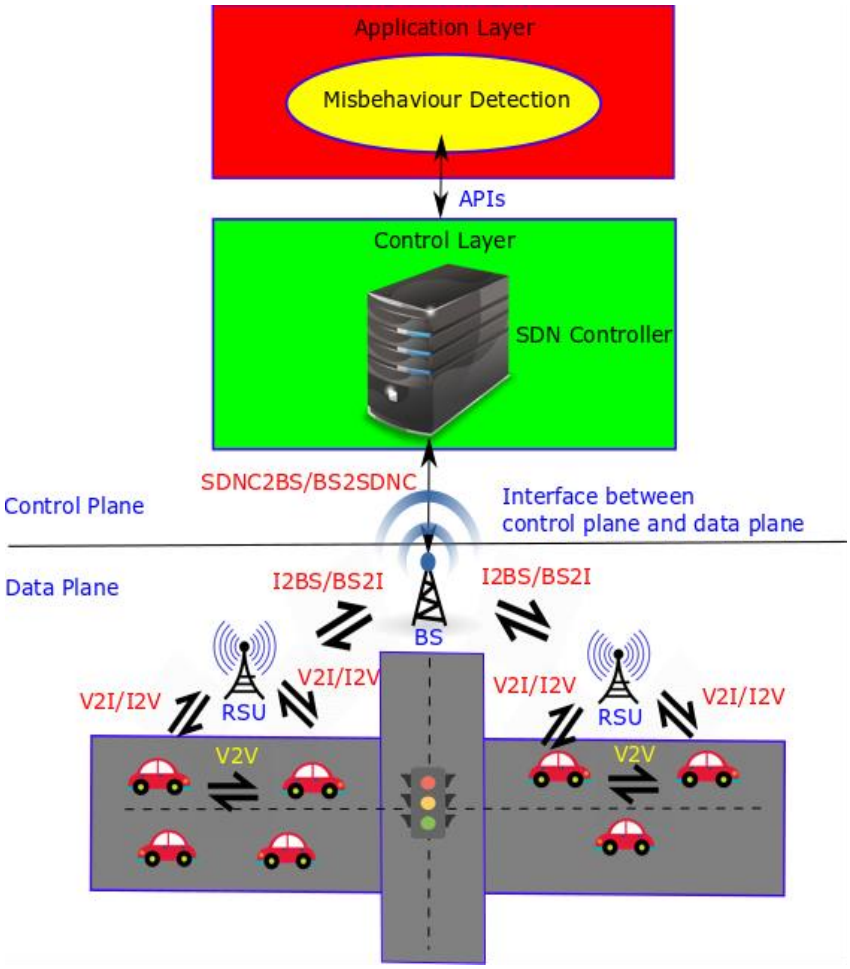

Fig. 2: An architecture of software defined vehicular network

4.2. Misbehavior Model

In this model, we have considered the Sybil misbehavior where a Sybil node or vehicle in the SDVN network creates fake identities to take control of the network. This is possible by creating unique fake identities and start beaconing from those identities to disrupt the network performance. These fake identities need to be detected. Fig. 3 presents the sybil misbehavior of vehicle V1 which creates fake identities such as V2 and V3. Afterwards V1 initiates beaconing from each vehicle to perform attack over the network such as routing attack, packet dropping, position cheating, etc. We assume that the Sybil node changes the parameters of the beacon message such as change of direction, change of current position, and change of speed. We also assume that the RSS of the Sybil nodes are same, as the beacons at a particular time are generated from a single Sybil node.

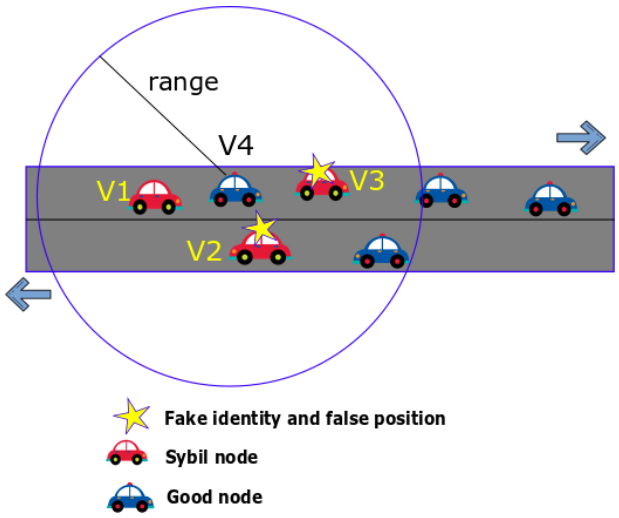

Fig. 3: Sybil misbehavior by the sybil node V1 in SDVN

4.3. Proposed Sybil Misbehavior Detection Approach

This section describes about the misbehavior detection approach for Sybil attack. From Fig. 3 it is observed that vehicle V1 is a Sybil node which creates the fake identities V2 and V3. V4 is a genuine vehicle which receives the beacon from V1 as well as V2 and V3 and stores it in the neighbor table. Let the beacon of V1 contains <V1, (x1,y1),sp1,dir1>. Similarly V2 and V3 beacons contain <V1,(x2,y2),sp2,dir2> and <V1,(x3,y3),sp2,dir2> respectively, where (x2,y2) and (x3,y3) are the virtual positions where actually vehicle does not lie. The steps to detect the Sybil nodes are described as follows.

Step 1: A vehicle checks which vehicles have the same RSS. The RSS of a neighbor vehicle is computed by the OBU.

Step 2: After finding the RSS of a neighbor vehicle, the distance drssi from which the signal is received is calculated by: -

$$drssi = 10^{\left(\frac{measured\ power - rssi}{10 \times N}\right)} \quad (1)$$

Where, measured power is calculated by a vehicle (V4) when beacon is received, rssi is the power at 1 m, and N is a constant which ranges from 2-4.

Step 3: After finding the drssi, it checks whether the distance d between itself (x1,y1) and neighbor vehicle (x2,y2) is same. If it is same, then the vehicle is assumed to be genuine else it is a fake identity vehicle and considered as Sybil node. The distance d is calculated using the Euclidean distance method shown as follows: -

$$d = sqrt((x2-x1)^2 + (y2-y1)^2) \quad (2)$$

Step 4: After finding the Sybil set, this sets information is forwarded to the SDNC using the simple position-based routing mechanism [1], for taking emergency action to keep the network safe from Sybil attackers.

The whole steps are clearly represented in the flowchart shown in Fig. 4. The algorithm is also presented in Algorithm 1. Step 2 to Step 5 has a time complexity of O(n), where n is the number of vehicles for which RSS is computed. Step 6 has O(n) time complexity where n vehicles RSS values are taken to find m vehicles with same RSS. Step 7 and Step 8 has complexity of O(1). Step 9 to Step 15 has complexity of O(m) where m is the number of vehicles with same RSS. Step 16 has a complexity of O(1) where the Sybil set information is send to SDNC.

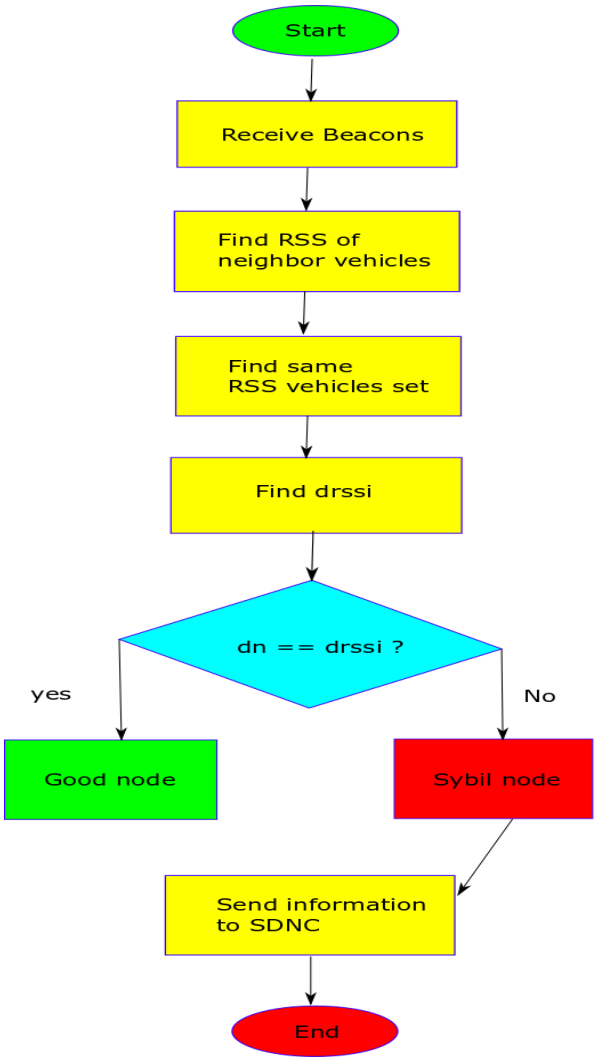

Fig. 4: Flowchart for Sybil misbehavior detection.

Algorithm 1: Sybil misbehavior detection in SDVN

Input: Beacon information of neighbour
Output: Sybil node

```
1.  Start
2.  For i=1:n                \\ n is the number of neighbour vehicles
                                3.  Compute RSSi;
4.      RSS[i] = RSSi;
5.  EndFor
6.  Cluster m with same RSS; \\ m is the number of vehicles with same
    RSS
7.  Calculate drssi; \\ drssi is same for the m vehicles
8.  k=0;
9.  For j=1:m
10.     Calculate dj;
11.     If (dj != drssi)
12.         Sybil[k]=j;
13.     EndIf
14. k=k+1;
15. EndFor
16. Send Sybil[] to SDNC;
17. End
```

5. SIMULATION AND RESULTS

To carry out the simulation, Veins hybrid framework simulator. IEEE 802.11p standard for communication by this simulator. In hybridization it uses OMNeT++ network simulator [30] and SUMO road traffic simulator [31]. These simulators are connected using a trace file interface. This interface provides the TCP connection and real time interaction between the network simulator and road traffic simulator. The simulation is performed in a grid scenario. The simulation setting is shown in Table 1 and Table 2 as follows. The results are the average of 20 simulation runs.

The performance of the proposed scheme is compared with Grover et al. [10] and Grover et al. [11] schemes which also uses the RSS based Sybil misbehavior detection approach. The performance parameters taken are: -

1. Detection accuracy: The number of misbehavior nodes detected correctly from the set of misbehavior nodes.
2. False Positive Rate (FPR): The number of good nodes incorrectly detected as Sybil nodes.
3. False Negative Rate (FNR): The number of Sybil nodes incorrectly detected as good nodes.
4. Detection time (DT): Time required to detect the Sybil nodes in the whole network.

Table 1: Simulation setting for SUMO

Sl. No.	Parameters	Values

1	Area	$3000 * 2000$ m^2
2	Number of Lanes	$3 *$ direction
3	Maximum Speed of Vehicles	30 m/s
4	Allowed Maximum Speed on Edges	30.556 m/s
5	Maximum Acceleration	3.0 m/s^2
6	Maximum Deceleration	6.0 m/s^2
7	Driver Imperfection	0.5
8	Number of vehicles	100
9	Vehicles type	3
10	Length of vehicle type	5 m, 7 m, 12 m

Table 2: Simulation setting for Network Simulator

Sl. No.	Parameters	Values
1	Simulation Time	300 s
2	Bitrate	6 Mbps
3	Packet Generation Rate	10 packets/s
4	Communication Range of Vehicle	300 m
5	Communication Range of RSU	500 m
6	Update Interval	0.1s
7	IEEE	802.11p
8	Sensitivity	-80 dBm
10	SDN controller	1
12	Number of RSU	4
13	BS	1
14	Number of simulation run	20

To evaluate the performance using the above performance parameters, the percentage of misbehaviors nodes are varied to see the change.

- Detection Accuracy: From Fig. 5 it is observed that detection accuracy reduces when the number of attackers increase in network. Proposed approach performs better in terms of detection accuracy by showing an average detection accuracy of 88%. Grover et al. [10] and Grover et al. [11] shows an average detection accuracy of 70% and 80.8%.

- FPR: From Fig. 6 it is observed that FPR reduces when the number of attackers increase in network. Proposed approach performs better in terms of FPR by showing an average

FPR of 3%. Grover et al. [10] and Grover et al. [11] shows an average FPR of 10% and 5.2%.

- FNR: From Fig. 7 it is observed that FNR increases when the number of attackers increase in network. Proposed approach performs better in terms of FNR by showing an average detection accuracy of 3%. Grover et al. [10] and Grover et al. [11] shows an average FNR of 10.4% and 5.2%.

- DT: From Fig. 8 it is observed that detection time increases when the number of attackers increase in network. Proposed approach performs better in terms of detection time by showing an average detection time of 30s. Grover et al. [10] and Grover et al. [11] shows an average detection time of 35s and 33s.

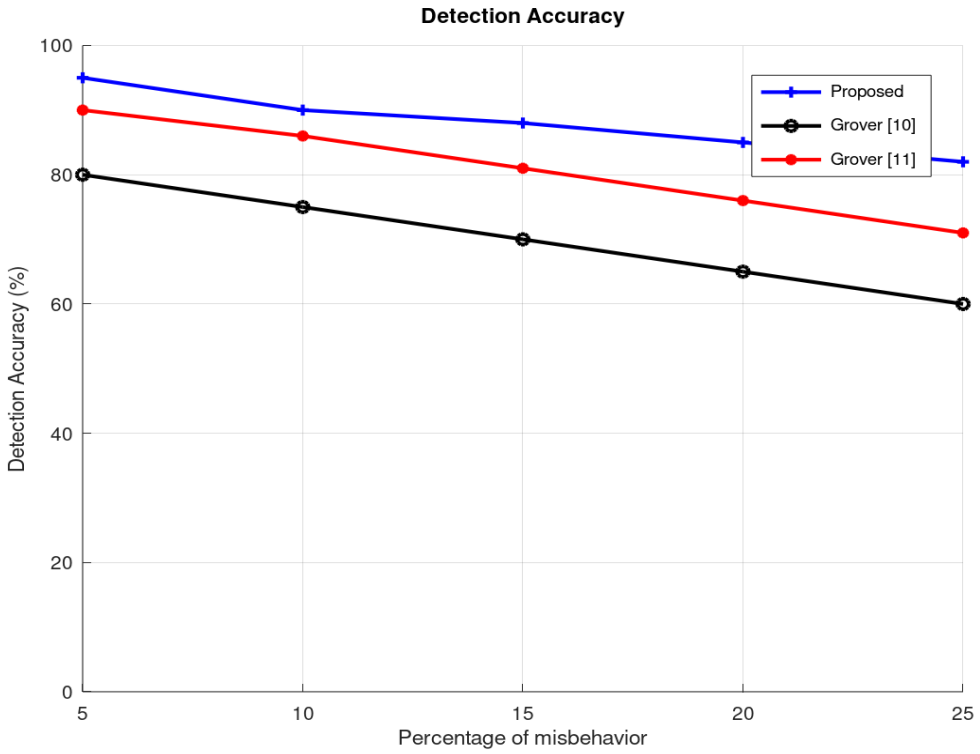

Fig. 5: Detection Accuracy

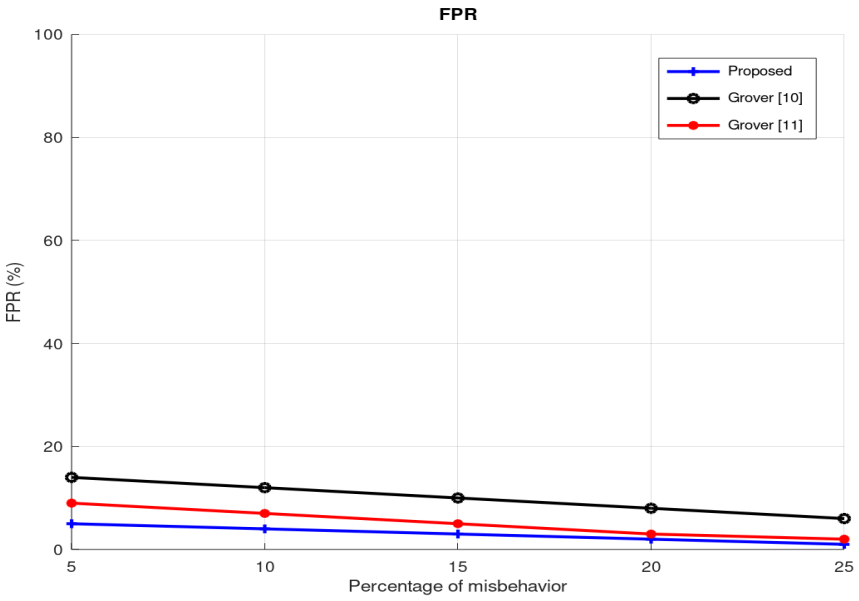

Fig. 6: False Positive Rate

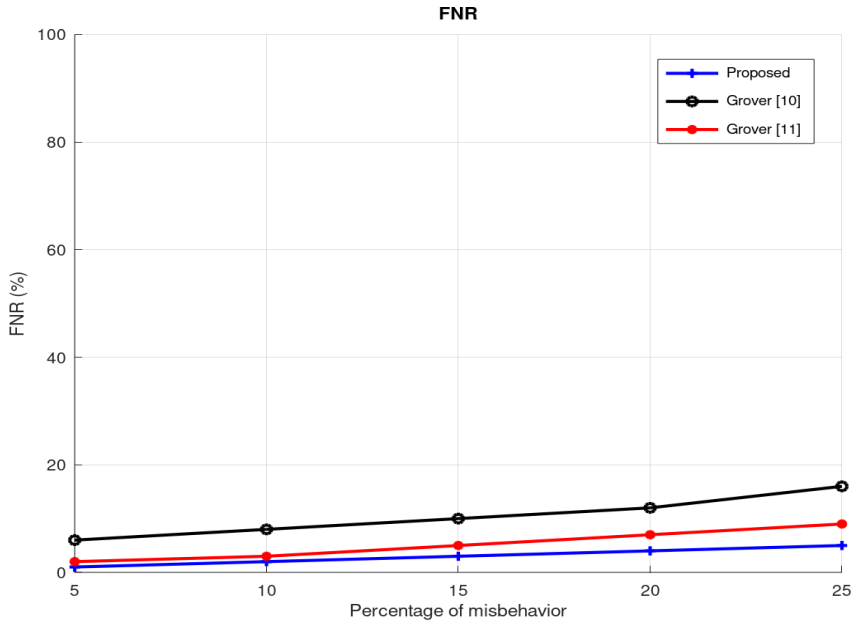

Fig. 7: False Negative Rate

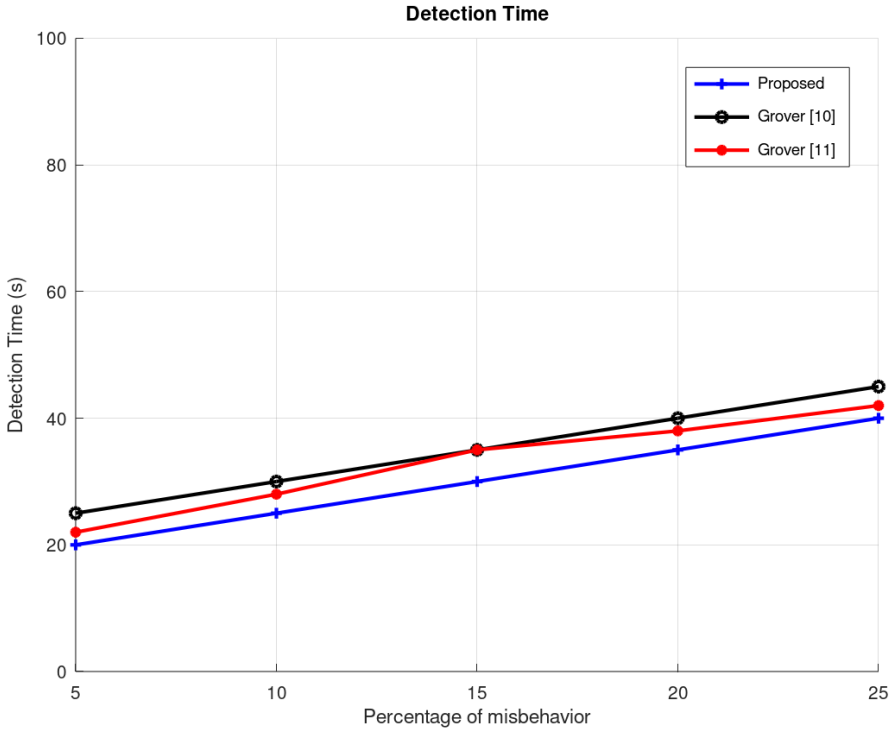

Fig. 8: Detection Time

6. CONCLUSION

Software-defined VANETs (SDVN) are a new research area where vehicular networks use the SDN technology for efficient network management. In this work, a Sybil misbehavior detection approach is proposed for SDVN using the RSS of a vehicle. The simulation of this proposed work is performed using OMNeT++ simulator and SUMO road traffic simulator. It is compared with other RSS based Sybil misbehavior detection schemes. From results it is observed that proposed approach performs better than above schemes in terms of detection accuracy, false positive rate, false negative rate, and detection time. This method will be better Sybil misbehavior detection approach in vehicular networks. In future, this method will be practically implemented by taking transceivers and SDN controller.

Acknowledgments

We want to thank GCE, Kalahandi, PMEC Berhampur, IGIT Sarang, and BPUT University, India for providing us the research infrastructure to carry out the work.

REFERENCES

[1] Bhoi, Sourav Kumar, and Pabitra Mohan Khilar. "Vehicular communication: a survey." IET networks 3, no. 3 (2013): 204-217.

[2] Sharef, Baraa T., Raed A. Alsaqour, and Mahamod Ismail. "Vehicular communication ad hoc routing protocols: A survey." Journal of network and computer applications 40 (2014): 363-396.

[3] Viriyasitavat, Wantanee, Mate Boban, Hsin-Mu Tsai, and Athanasios Vasilakos. "Vehicular communications: Survey and challenges of channel and propagation models." IEEE Vehicular Technology Magazine 10, no. 2 (2015): 55-66.

[4] Engoulou, Richard Gilles, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. "VANET security surveys." Computer Communications 44 (2014): 1-13.

[5] Hasrouny, Hamssa, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. "VANet security challenges and solutions: A survey." Vehicular Communications 7 (2017): 7-20.

[6] Khan, Uzma, Shikha Agrawal, and Sanjay Silakari. "A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks." In Information systems design and intelligent applications, pp. 11-19. Springer, New Delhi, 2015.

[7] Ku, Ian, You Lu, Mario Gerla, Rafael L. Gomes, Francesco Ongaro, and Eduardo Cerqueira. "Towards software-defined VANET: Architecture and services." In 2014 13th annual Mediterranean ad hoc networking workshop (MED-HOC-NET), pp. 103-110. IEEE, 2014.

[8] Truong, Nguyen B., Gyu Myoung Lee, and Yacine Ghamri-Doudane. "Software defined networking-based vehicular adhoc network with fog computing." In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 1202-1207. Ieee, 2015.

[9] Arif, Muhammad, Guojun Wang, Oana Geman, Valentina Emilia Balas, Peng Tao, Adrian Brezulianu, and Jianer Chen. "Sdn-based vanets, security attacks, applications, and challenges." Applied Sciences 10, no. 9 (2020): 3217.

[10] Grover, Jyoti, M. S. Gaur, Nitesh Prajapati, and Vijay Laxmi. "RSS-based Sybil attack detection in VANETs." In Proceedings of the international conference TENCON2010, IEEE, pp. 2278-2283. 2010.

[11] Grover, Jyoti, Manoj Singh Gaur, Vijay Laxmi, and Nitesh Kumar Prajapati. "A sybil attack detection approach using neighboring vehicles in VANET." In Proceedings of the 4th international conference on Security of information and networks, pp. 151-158. 2011.

[12] Grover, Jyoti, Manoj Singh Gaur, and Vijay Laxmi. "Multivariate verification for sybil attack detection in VANET." Open Computer Science 5, no. 1 (2015): 60-78.

[13] Grover, Jyoti, Manoj Singh Gaur, and Vijay Laxmi. "A novel defense mechanism against sybil attacks in VANET." In Proceedings of the 3rd international conference on Security of information and networks, pp. 249-255. 2010.

[14] Grover, Jyoti, Vijay Laxmi, and Manoj Singh Gaur. "Sybil attack detection in VANET using neighbouring vehicles." International Journal of Security and Networks 9, no. 4 (2014): 222-233.

[15] Park, Soyoung, Baber Aslam, Damla Turgut, and Cliff C. Zou. "Defense against sybil attack in vehicular ad hoc network based on roadside unit support." In MILCOM 2009-2009 IEEE Military Communications Conference, pp. 1-7. IEEE, 2009.

[16] Hussain, Rasheed, and Heekuck Oh. "On secure and privacy-aware sybil attack detection in vehicular communications." Wireless personal communications 77, no. 4 (2014): 2649-2673.

[17] Rajadurai, Hariharan, and Usha Devi Gandhi. "Fuzzy based collaborative verification system for Sybil attack detection in MANET." Wireless Personal Communications 110, no. 4 (2020): 2179-2193.

[18] Abbas, Sohail, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat. "Lightweight sybil attack detection in manets." IEEE systems journal 7, no. 2 (2012): 236-248.

[19] Kushwaha, Deepak, Piyush Kumar Shukla, and Raju Baraskar. "A survey on Sybil attack in vehicular ad-hoc network." International Journal of Computer Applications 98, no. 15 (2014).

[20] Kumar Karn, Chaitanya, and Chandra Prakash Gupta. "A survey on VANETs security attacks and sybil attack detection." International Journal of Sensors Wireless Communications and Control 6, no. 1 (2016): 45-62.

[21] Shrestha, Rakesh, Sirojiddin Djuraev, and Seung Yeob Nam. "Sybil attack detection in vehicular network based on received signal strength." In 2014 International Conference on Connected Vehicles and Expo (ICCVE), pp. 745-746. IEEE, 2014.

[22] Park, Soyoung, Baber Aslam, Damla Turgut, and Cliff C. Zou. "Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support." Security and Communication Networks 6, no. 4 (2013): 523-538.

[23] Muhamad, Aveen, and Mourad Elhadef. "Sybil attacks in intelligent vehicular ad hoc networks: A review." Advanced Multimedia and Ubiquitous Engineering (2018): 547-555.

[24] Faisal, Mohammad, Sohail Abbas, and Haseeb Ur Rahman. "Identity attack detection system for 802.11-based ad hoc networks." EURASIP Journal on Wireless Communications and Networking 2018, no. 1 (2018): 1-16.

[25] Saggi, Mandeep Kaur, and Ranjeet Kaur. "Isolation of Sybil attack in VANET using neighboring information." In 2015 IEEE International Advance Computing Conference (IACC), pp. 46-51. IEEE, 2015.

[26] Yang, Jie, Yingying Chen, and Wade Trappe. "Detecting sybil attacks inwireless and sensor networks using cluster analysis." In 2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 834-839. IEEE, 2008.

[27] Gamal, Manal S., Abdurrahman A. Nasr, and Sayed A. Nouh. "Vanet security: Defense and detection, A review." Journal of Al-Azhar University Engineering Sector 15, no. 56 (2020): 810-827.

[28] Wang, Chundong, Likun Zhu, Liangyi Gong, Zhentang Zhao, Lei Yang, Zheli Liu, and Xiaochun Cheng. "Accurate sybil attack detection based on fine-grained physical channel information." Sensors 18, no. 3 (2018): 878.

[29] Khalil, Mohamed, and Marianne A. Azer. "Crypto-SAP Protocol for Sybil Attack Prevention in VANETs." In Advances in Computer, Communication and Computational Sciences, pp. 143-152. Springer, Singapore, 2021.

[30] https://omnetpp.org/, accessed on April 2021.

[31] https://www.eclipse.org/sumo/, accessed on April 2021.

[32] Sahoo, Kshira Sagar, and Deepak Puthal. "SDN-Assisted DDoS Defense Framework for the Internet of Multimedia Things." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 16.3s (2020): 1-18.

[33] Nithya, S., et al. "SDCF: A software-defined Cyber Foraging Framework for Cloudlet Environment." IEEE Transactions on Network and Service Management 17.4 (2020): 2423-2435.

[34] Mishra, Sambit Kumar, et al. "Energy-aware task allocation for multi-cloud networks." IEEE Access 8 (2020): 178825-178834.

[35] S. J. Hussain, U. Ahmed, H. Liaquat, S. Mir, N. Jhanjhi and M. Humayun, "IMIAD: Intelligent Malware Identification for Android Platform," 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1-6, doi: 10.1109/ICCISci.2019.8716471.

[36] Lee, S., Abdullah, A., Jhanjhi, N., & Kok, S. (2021). Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning. PeerJ Computer Science, 7, e350.

[37] Hussain, K., Jhanjhi, N. Z., Mati-ur-Rahman, H., Hussain, J., & Islam, M. H. (2019). Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes. Journal of King Saud University-Computer and Information Sciences.

[38] F. A. Almusalli, N. Zaman and R. Rasool, "Energy efficient middleware: Design and development for mobile applications," 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 541-549, doi: 10.23919/ICACT.2017.7890149.

[39] Navid Ali Khan, Noor Zaman Jhanjhi, Sarfraz Nawaz Brohi, Anand Nayyar, Chapter Three - Emerging use of UAV's: secure communication protocol issues and challenges, Editor(s): Fadi Al-Turjman, Drones in Smart-Cities, Elsevier, 2020, Pages 37-55, ISBN 9780128199725,

[40] Lim M, Abdullah A, Jhanjhi N, Supramaniam M. Hidden Link Prediction in Criminal Networks Using the Deep Reinforcement Learning Technique. Computers. 2019; 8(1):8. https://doi.org/10.3390/computers8010008

[41] Hussain, K., Hussain, S. J., Jhanjhi, N. Z., & Humayun, M. (2019, April). SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-4). IEEE.