ODPV: An Efficient Protocol to Mitigate Data Integrity Attacks in Intelligent Transport Systems

Javed, M. A., Khan, M. Z., Zafar, U., Siddiqui, M. F., Badar, R., Lee, B. M. & Ahmad, F.

Original citation:
Javed, MA, Khan, MZ, Zafar, U, Siddiqui, MF, Badar, R, Lee, BM & Ahmad, F 2020, 'ODPV: An Efficient Protocol to Mitigate Data Integrity Attacks in Intelligent Transport Systems', IEEE Access, vol. 8, pp. 114733-114740.
https://dx.doi.org/10.1109/ACCESS.2020.3004444

DOI 10.1109/ACCESS.2020.3004444
ESSN 2169-3536

Publisher: Institute of Electrical and Electronics Engineers

IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received June 11, 2020, accepted June 20, 2020, date of publication June 23, 2020, date of current version July 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004444

ODPV: An Efficient Protocol to Mitigate Data Integrity Attacks in Intelligent Transport Systems

MUHAMMAD AWAIS JAVED[1], (Senior Member, IEEE), MOHAMMAD ZUBAIR KHAN[2], USMAN ZAFAR[1], MUHAMMAD FAISAL SIDDIQUI[1], RABIAH BADAR[1], BYUNG MOO LEE[3], (Member, IEEE), AND FARHAN AHMAD[4], (Member, IEEE)

[1]Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad 45550, Pakistan
[2]Department of Computer Science, College of Computer Science and Engineering, Taibah University, Madinah 41477, Saudi Arabia
[3]School of Intelligent Mechatronics Engineering, Sejong University, Seoul 05006, South Korea
[4]Cyber Security Research Group, College of Engineering and Technology, University of Derby, Derby DE22 1GB, U.K.

Corresponding authors: Muhammad Awais Javed (awais.javed@comsats.edu.pk), Mohammad Zubair Khan (mkhanb@taibahu.edu.sa), and Byung Moo Lee (blee@sejong.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Korea Government Ministry of Science and ICT (MSIT) under Grant NRF-2020R1F1A1048470 and Grant NRF-2019R1A4A1023746.

ABSTRACT Intelligent Transport Systems (ITS) require accurate information to be shared among vehicles and infrastructure nodes for applications including accident information or pre-crash warnings, to name a few. Due to its sensitive nature, ITS applications are vulnerable against data integrity attacks where nodes transmit false information that results in wrong decision making by the applications. A characteristic of such attacks is that the false transmitted information is significantly different than the actual information. In this paper, we propose an Outlier Detection, Prioritization and Verification (ODPV) protocol that efficiently isolates false data and improves traffic management decisions. ODPV uses the isolation forest algorithm to detect outliers, fuzzy logic to prioritize outliers and C-V2X communications to verify the outliers. Extensive simulation results verify the effectiveness of the proposed protocol to isolate the outliers.

INDEX TERMS Data integrity, intelligent transport systems, vehicular network.

I. INTRODUCTION

As the cities are expanded with the growing population, people frequently travel long distances for work and other purposes. Intelligent Transportation Systems (ITS) are thus a major need of the present to improve traffic management and reduce traveling times [1]–[3]. Future smart cities will effectively solve traffic issues such as accidents, timely emergency notification issuance, and congestion on the road [4]–[6].

Wireless connectivity between vehicles provides a potential solution to major transportation problems [7]–[9]. Wireless-enabled automobiles along with the infrastructure components on the road are linked with the traffic management centers that use intelligent data analysis tools to efficiently manage city traffic and improve traffic flow. The transportation system is progressively moving toward electric, autonomous and intelligent vehicles [10].

The associate editor coordinating the review of this manuscript and approving it for publication was Huan Zhou.

The major components of future ITS include the On-board Units (OBUs) that are devices fitted at the vehicles to communicate to other OBUs or infrastructure units [11]. Another important component of ITS is the Road Side Units (RSUs) that are wireless devices installed at various places on the road. RSUs can transmit and receive data to/from the OBUs [12], [13]. RSUs provide OBUs with information such as traffic services (traffic congestion measurement, accident notification, and road conditions), infotainment and advertisements. The last component of ITS is the Traffic Command Center (TCC) which is connected to all RSUs and manages city-wide data.

Although the wireless connectivity provided by the ITS improves safety and traffic management, security attacks could negatively impact the performance of various applications [14]. Thus, the privacy and security of data shared among the different components of ITS is an important technical task [13], [15]. Malicious nodes could cause great security risk as most ITS applications involve human safety. So, it is important to ensure integrity, authenticity, trust, non-repudiation, and confidentiality of data shared among ITS components for all applications [16]–[19].

Of the many security challenges faced by the ITS, reliability of data shared among ITS components is a vital challenge [20], [21]. ITS applications are subject to data integrity attacks where malicious vehicles can transmit wrong information regarding surrounding vehicle density and emergency events [4], [14], [22]. This could badly impact safety applications as well as traffic management applications, resulting in wrong decision making by the applications. As an example, the sharing of wrong vehicle density information or the generation of false accident alarms can cause traffic congestion.

To mitigate such data integrity attacks, RSUs need to analyze the received data from the vehicles for potential accuracy. The false information or outlier such as wrong traffic density information should be detected by the RSUs and verified (to confirm if it is malicious information or an actual data) from other vehicles in the vicinity by using the minimum number of communication resources. So, two major challenges to mitigate data integrity attacks include outlier detection and outlier verification.

The major contributions of this paper are

- We propose an Outlier Detection, Prioritization and Verification (ODPV) protocol that detects outliers in the traffic density information using isolation forest algorithm.
- ODPV ranks the detected outliers in terms of their criticality based on a proposed fuzzy logic algorithm.
- ODPV optimizes the use of C-V2X sub-channels by verifying the most critical outliers first.
- Simulation results show that ODPV effectively detects outliers with accuracy and utilizes the sub-channels effectively to verify the most critical outliers.

The rest of the paper is organized as follows. Section II presents the related works followed by the working of the proposed ODPV in Section III. Section IV presents the performance evaluation of the proposed protocol. Conclusions are drawn in Section V.

II. RELATED WORKS

In this section, comprehensive literature review related to outlier detection and data integrity attacks is discussed. In [14], the authors proposed a forged data filtering scheme to mitigate the data integrity attacks in route guidance applications. The authors discussed the security challenges of the route guidance method used in the ITS. In this scheme, forged data filtering (FDF) is used to authenticate the received data by using ternary polynomials. FDF is the message validation algorithm for ITS, which generates the message authentication codes to check the validity of the forwarded data. The forged data of traffic states can be efficiently filtered out during the data transfer in vehicular networks. This work achieves better data integrity, as polynomial authentication is hard to break, at the cost of high authentication delay and high hardware cost.

In [2], authors proposed a Dynamic En-route Decision real-time Route guidance (DEDR) scheme to efficiently mitigate the congestion on the roads produced by the unexpected increase of automobiles, which eventually decreases the travel time and reduces the fuel consumption. DEDR takes the knowledge of real-time traffic by using vehicular networks. This real-time shared traffic data allows DEDR to introduce the trust probability, which helps to predict traffic situation and to dynamically determine the alternative best possible routes. DEDR scheme also enhances the real-time decision capability of the driver in terms of optimal route selection, by providing different traffic congestion quantifying metrics.

In [23], the authors tackle the task of designing a Visual Analytics (VA) based ITS framework. which supports the examination of traffic data of road to detect anomalous behavior. Analysis of huge amounts of traffic data for detecting anomaly is a difficult task. VA can link the gap between human and computational approaches to detect anomalous actions in road traffic, building the data investigation process transparent. Authors presented a VA framework that offers support for: 1) Multidimensional traffic data exploration; 2) Analysis of communication models constructed from data; 3) Anomalous events detection, and 4) the explanations of the anomalous events.

In [24], the authors proposed an attack-resistant trust management scheme called ART. This scheme is proposed to deal with malicious attacks and assesses the reliability of reported data and nodes in VANETs. In the ART mechanism, the authors model the reliability of data and nodes as two different metrics, named data trust and node trust, respectively. In specific, the authors used data trust to evaluate the authenticity of the reported traffic data or to what extent the given traffic data are reliable. On the contrary, node trust shows how reliable the nodes in VANETs are. Furthermore, the ART scheme is able to detect malicious nodes in VANETs.

In [25], the authors presented K-Nearest Neighbors (KNN) technique to detect outliers in the daily collected large-scale traffic data of the city. Outliers contain data errors, hardware errors and abnormal traffic activities. The given kNN technique detects outliers by checking the relationship between data points in the neighborhood. In [26], the authors proposed an Outlier Detection using Indegree Number (ODIN) algorithm that uses the graph theory approach along with the KNN technique. Metrics such as node indegree number and average KNN distance is used to classify the outliers.

III. SYSTEM MODEL

We present the system model in this section. As shown in Fig. 1, we consider a scenario where vehicles periodically share traffic messages (containing information about vehicle speed, vehicle position, and vehicle density) and also with the infrastructure RSUs. Based on these traffic messages, RSUs estimate the traffic density in the neighborhood and feeds this information to the route guidance application in the city traffic command center.

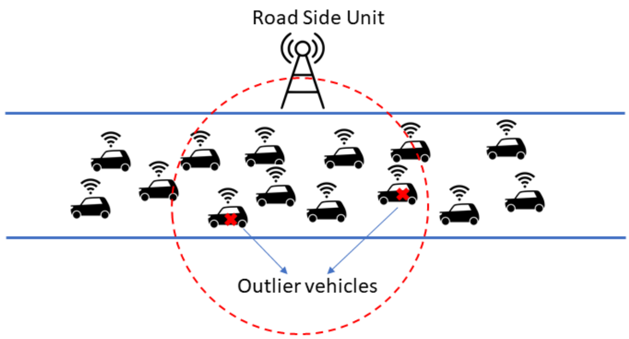


FIGURE 1. Outlier vehicles within the communication range of RSU.

Since the communication range of RSU is limited, it relies on the vehicle density information received by the vehicles within its range to estimate the neighborhood vehicle density. Note that the vehicles periodically share Cooperative Awareness Messages (CAM) with the neighboring vehicles, and have an estimate of the surrounding vehicle density based on the number of CAMs received. Particularly, the vehicles at the edge of the RSU's communication range are critical as they provide an estimate of the vehicle density outside the communication range of RSU.

As shown in Fig. 1, we consider that few of the vehicles within the communication range of RSU are malicious (we call them outlier vehicles in this paper) sending wrong vehicle density information. If the RSU considers the information by these outlier vehicles for traffic density estimation, it may result in erroneous traffic management decisions.

IV. PROPOSED ODPV PROTOCOL

To mitigate data integrity attacks in ITS, we propose an Outlier Detection, Prioritization and Verification (ODPV) protocol in this section. ODPV protocol works in three steps to improve the reliability of traffic information messages as shown in Fig. 2. In the first step, the ODPV protocol detects the outlier vehicles using the Isolation Forest algorithm. This is followed by a fuzzy logic-based outlier prioritization algorithm. The final step of the ODPV protocol is the outlier verification using neighborhood vehicles. Vehicle density reported by the outlier vehicles is only used for traffic management if it can be successfully verified. In the following, we explain the three steps of the ODPV protocol in detail.

A. OUTLIER DETECTION

In the *Outlier Detection* step, the RSU takes the vehicle density values received from all the vehicles and apply the Isolation Forest algorithm [27] to detect the outliers. Most of the existing techniques to detect outliers make a profile of the normal cases and then select the cases that do not follow the normal profile as outliers or anomalies. In comparison, Isolation Forest is unique in the way that it isolates the outliers by random partitioning of the data set. Since outliers are generally significantly different in value than the normal points, they can be isolated with a lower number of partitions.

TABLE 1. Fuzzy logic table.

Fuzzy Inputs		Fuzzy Output
Distance from RSU d_{rsu}	**Received Power P_r**	**Outlier Priority Level**
High	High	8
	Medium	7
	Low	6
Medium	High	5
	Medium	4
	Low	3
Low	High	2
	Medium	1
	Low	0

This idea can be explained in Fig. 3 where a normal value such as x_0 takes 6 partitions to get isolated. On the other hand, an outlier such as x_1 can be isolated with a single partition.

Isolation Forest produces multiple trees to build a forest. To generate a single tree, a sample of the data is first obtained. Then, one of the dimensions (x or y) is randomly selected and a random value is picked along that dimension. The data is split by drawing a straight line at the random value as shown in Fig. 3. As a result, a tree is formed as shown in Fig. 4. Multiple numbers of these trees constitute the forest. The two important parameters of the Isolation Forest algorithm are the number of trees and the size of the data sample.

Based on the developed forest, path length values of the tree are computed. Path length $p(n)$ of a data sample of size n is defined as the number of edges required to reach the selected point in a tree from the root node. As in Fig. 4, the path length to reach x_0 is 6. Path length is converted to an Anomaly score $A(x, n)$ as follows:

$$A(x, n) = 2^{\frac{-E(p(x))}{f(n)}} \tag{1}$$

where $E(p(x))$ is the average of $p(x)$ computed from multiple trees and $f(n)$ is the average of $p(x)$ when the search for x is unsuccessful.

B. OUTLIER PRIORITIZATION

The second step of ODPV protocol is *Outlier Prioritization* which uses fuzzy logic to rank the outliers in terms of their criticality. We use two parameters namely received power P_r and distance from the RSU d_{rsu} to sort the outliers. The proposed fuzzy logic table is given in Table 1. Fuzzy inputs are P_r and d_{rsu} which are categorized into three levels each. Fuzzy output is the priority level of the outliers ranging from 0 to R_{max}. Here R_{max} represents the highest priority level which is given to the most critical outliers.

As shown in Table 1, vehicles that have a high value of d_{rsu} and a high value of P_r are given the highest outlier priority level. This is because the RSU relies on the vehicles at the edge of its communication range to get the information (about the vehicle density) of the vehicles outside its communication range. Moreover, if the received power of the message is also

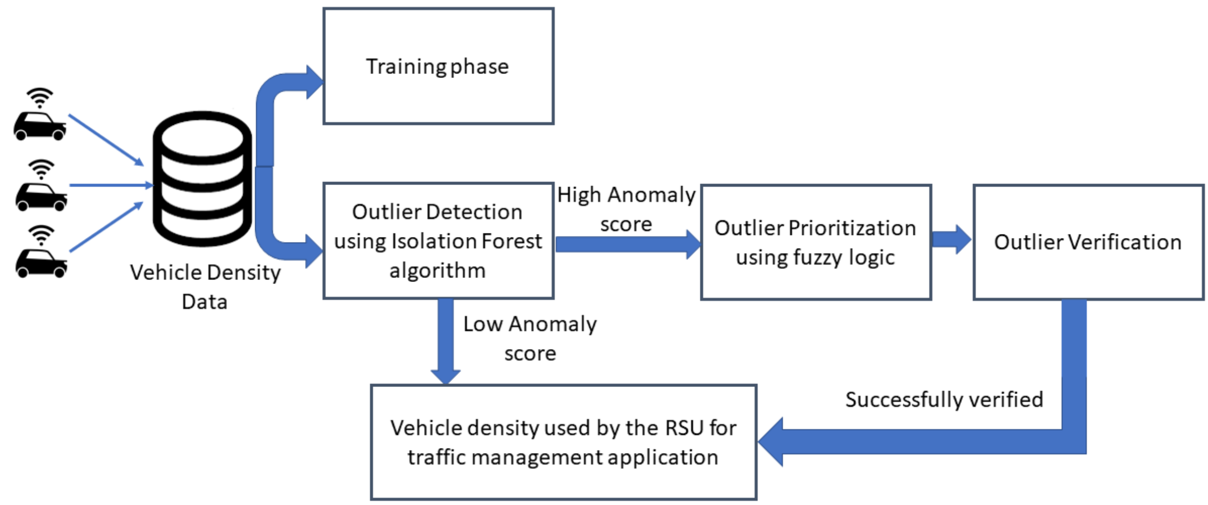


FIGURE 2. Working of proposed ODPV protocol.

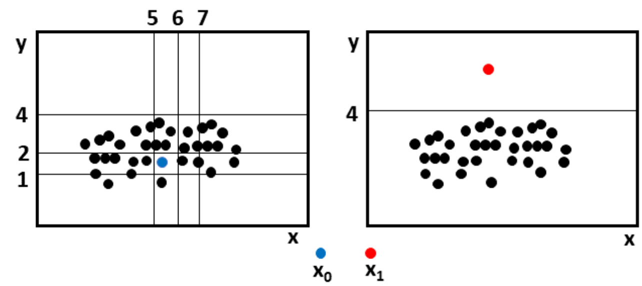


FIGURE 3. Working of isolation forest algorithm.

high, this means that the edge vehicle currently has good channel conditions and its vehicle density estimate is not erroneous due to multi-path fading. This means that there is a high chance that the value reported by the vehicle is malicious. So, this outlier must be verified first. Similarly, we prioritize the outliers using these two parameters and rank them as shown in Table 1.

C. OUTLIER VERIFICATION

In the third step named as *Outlier Verification*, ODPV protocol verifies the outliers by sending a verification message to a vehicle closer to the outlier vehicle. The verification vehicle v is selected as the one which is within a distance d_{max} of the outlier vehicle and not detected as an outlier (as part of the first step of the ODPV protocol). If there is no non-outlier vehicle within d_{max} of the outlier vehicle, then a vehicle with the least outlier priority is selected as the verification vehicle. This is done to ensure that a malicious vehicle is not selected as the verification vehicle.

In case the outlier vehicle is near the edge of the RSU and there is no non-outlier vehicle within its d_{max}, then we select the vehicle with the least outlier priority as the relay vehicle. A multi-hop verification message is then sent to a vehicle outside the communication range of the RSU using the relay vehicle. This is done to confirm if the reported vehicle density value by the edge vehicle is an outlier or not. After receiving the verification message, the verification vehicle v sends its vehicle density information to the RSU using the relay vehicle. If the vehicle density is not close to the outlier vehicle's reported vehicle density, then the outlier vehicle is marked as malicious. Furthermore, information received from the malicious vehicles is not used for vehicle density estimation at the RSU as shown in Fig. 2.

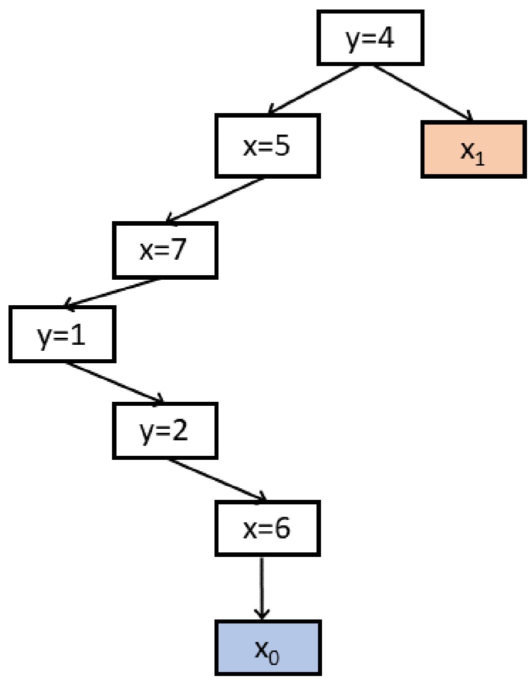
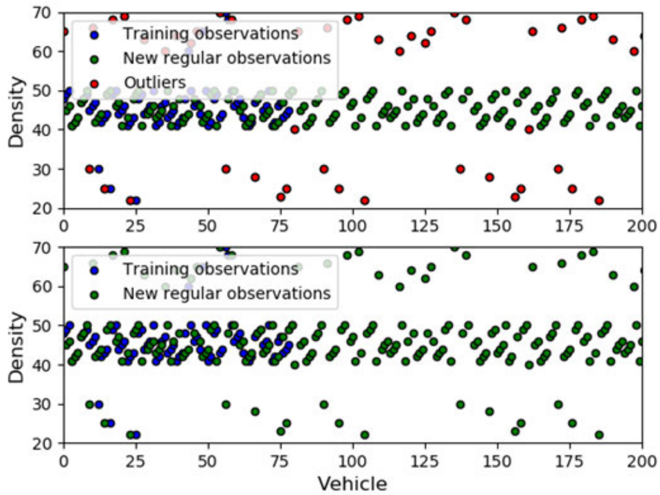


FIGURE 4. Development of tree using isolation forest algorithm.

V. PERFORMANCE EVALUATION

We present the performance evaluation of the proposed ODPV protocol in this section. We developed a simulation model in Python for a highway scenario with 2 lanes. We used



(a) Medium density scenario

(b) High density scenario

FIGURE 5. Training, outliers and real-time data of vehicle densities.

TABLE 2. Simulation parameters.

Parameter	Value
Vehicle Density	25 − 50 vehicles/km
Number of Lanes	2
Transmission Range	500m
Path loss exponent	3
Outlier vehicles ratio	0.1
Maximum number of samples in Isolation forest algorithm	40
Data set contamination in Isolation forest algorithm	0.1

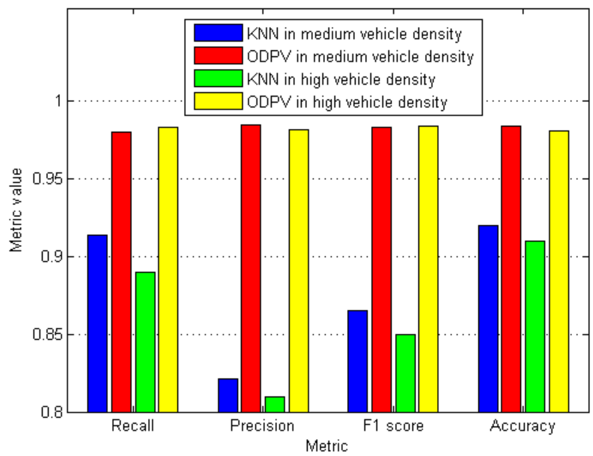


FIGURE 6. Recall, precision, F1 score and accuracy metric values for ODPV protocol and k-nearest algorithm.

two levels of vehicle densities, medium and high, where medium and high corresponds to a vehicle density of 25 vehicles/km and 50 vehicles/km. Vehicles are equipped with C-V2X transceivers and have a transmission range of 500m. The path loss exponent is taken as 3. We randomly select the number of outliers as 10% of the total number of vehicles. For the isolation forest algorithm, we use the maximum number of samples and data set contamination parameters as 40 and 0.1 respectively. Simulation parameters are listed in Table 2.

We show the vehicle densities reported by the vehicles to the RSU in both medium and high-density scenarios in Fig. 5. Initially, these vehicle density values are used to train the RSU for normal values. After the training phase, we apply the ODPV protocol on different mobility traces of medium and high density to detect the outliers. One sample of new regular observations is seen in Fig. 5. Results show that the ODPV protocol efficiently detects the outliers marked in red color in in Fig. 5. The isolation forest algorithm used in ODPV effectively isolates the abnormal values from the normal vehicle density values.

We present the results of isolation forest outlier detection performance of OPDV protocol in Fig. 6. We compare the proposed OPDV protocol with the K-Nearest Neighbors (KNN) algorithm in [25]. The results are presented in terms of four common metrics defined as follows:

- **Recall** is defined as the number of true positives divided by the sample size.

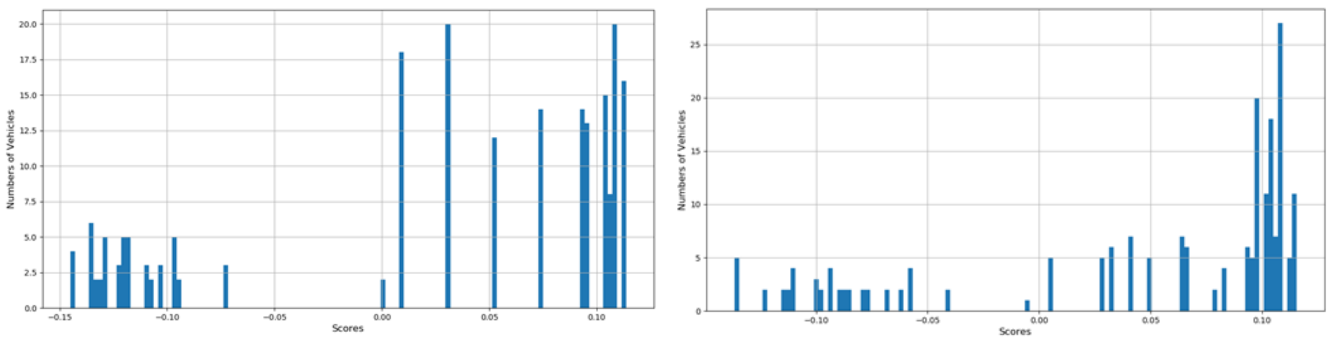
$$Recall = \frac{TP}{TP + FN} \tag{2}$$

where TP is the number of true positives, and FN is the number of false negatives.

- **Precision** is defined as the the number of correctly classified positive results divided by the number of results labeled by the system as positive.

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

where FP is the number of false positives.



(a) Medium density scenario

(b) High density scenario

FIGURE 7. **Anomaly scores.**

- **F1 score** is a measure of the accuracy by considering both the precision and the recall.

$$F1\ score = \frac{2 \times Recall \times Precision}{Recall + Precision} \tag{4}$$

- **Accuracy** is fraction of predicted results which are correct among all the cases.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

where TN is the number of true negatives.

As can be seen from Fig. 6, isolation forest algorithm of the ODPV protocol scores more than 0.98 in all of the above metrics. This shows that the isolation forest algorithm has a robust performance in the context of ITS and can be used to detect outliers and malicious vehicles. On the other hand, KNN algorithm provides a recall of more than 0.88, however, its precision is 0.82 for medium vehicle density. The reason for low precision value in KNN is the high number of false positives. This occurs because only K nearest neighbors are considered for detecting an outlier and algorithm finds a positive outlier if any change in vehicle density exists among those K neighbors. Also, KNN algorithm does not have a verification procedure. Similarly, F1 score and accuracy of KNN is up to 15% less than the OPDV protocol.

In Fig. 7, we show the number of vehicles with a particular anomaly score for both medium and high-density scenarios. Anomaly score gives us information about the inliers and the outliers. The lower the anomaly score of the data instances, the more abnormal the data. Negative anomaly scores represent the outliers and the positive scores represent the inliers.

We show the number of outliers with a particular priority level in Fig. 9. It can be seen that ODPV prioritizes the outliers in terms of their criticality. It can be seen that less than half of the outliers are ranked higher than 4 and this prioritization helps verify the most critical outliers first.

The number of sub-channels required to verify the outliers of each priority level is shown in Fig. 9. These sub-channels are computed based on the single-hop and the multi-hop communications as proposed by the *Outlier Verification* algorithm of the ODPV protocol. For outliers with the priority

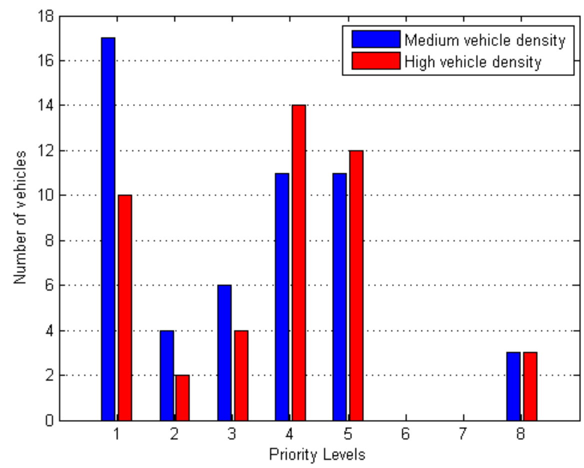


FIGURE 8. **Number of vehicles at different outlier levels in medium and high density scenarios.**

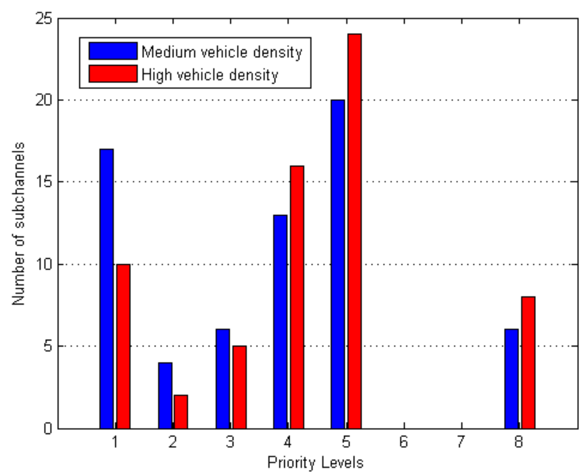


FIGURE 9. **Number of sub-channels required in medium and high density scenarios.**

level of 8, ODPV protocol requires 7 sub-channels whereas, for the outliers with a priority level of 5, 23 sub-channels are needed in a high vehicle density scenario.

Fig. 10 shows the number of outliers that are verified with a particular priority level based on the available free

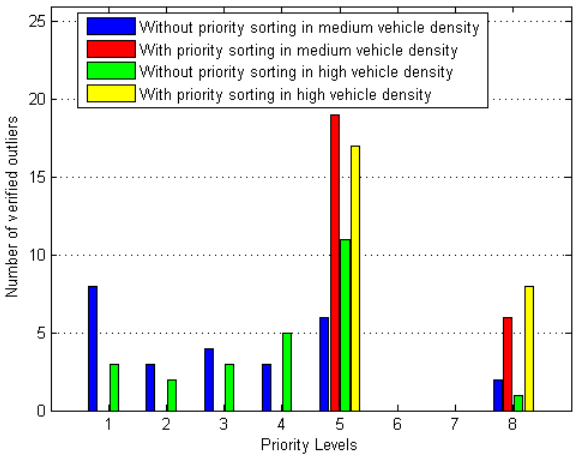


FIGURE 10. Number of outliers that are verified with sorting and without priority sorting in medium and high density scenarios.

sub-channels. It can be seen that the priority sorting algorithm of ODPV manages to verify all the outliers with a priority level of equal to or higher than 4. In contrast, without priority sorting, the outliers are randomly picked for verification and many critical outliers could not be verified. Therefore, the proposed ODPV protocol efficiently utilizes the sub-channels to verify the most critical outliers.

VI. CONCLUSION

Data integrity attacks could severely limit the reliability of ITS applications. In this paper, we propose the ODPV protocol that mitigates such attacks by detecting outliers using an isolation forest algorithm. Furthermore, ODPV uses fuzzy logic to prioritize outliers in terms of their severity and verifies the reported outliers from the neighborhood vehicles. Simulation results show the robust performance of the ODPV protocol to efficiently detect and verify the outliers using C-V2X communications.

REFERENCES

[1] F. Jameel, S. Wyne, M. A. Javed, and S. Zeadally, "Interference-aided vehicular networks: Future research opportunities and challenges," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 36–42, Oct. 2018.

[2] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, "A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2551–2566, Mar. 2017.

[3] M. A. Javed and S. Zeadally, "RepGuide: Reputation-based route guidance using Internet of vehicles," *IEEE Commun. Standards Mag.*, vol. 2, no. 4, pp. 81–87, Dec. 2018.

[4] M. A. Javed, S. Zeadally, and E. B. Hamida, "Data analytics for cooperative intelligent transport systems," *Veh. Commun.*, vol. 15, pp. 63–72, Jan. 2019.

[5] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Sep. 2017.

[6] Y. Cao, T. Jiang, O. Kaiwartya, H. Sun, H. Zhou, and R. Wang, "Toward pre-empted EV charging recommendation through V2 V-based reservation system," *IEEE Trans. Syst., Man, Cybern. Syst.*, early access, Jun. 11, 2019, doi: 10.1109/TSMC.2019.2917149.

[7] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, and L. Zhao, "Vehicle-to-everything (v2x) services supported by LTE-based systems and 5G," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 70–76, Jun. 2017.

[8] R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, Dec. 2017.

[9] M. A. Javed, N. S. Nafi, S. Basheer, M. Aysha Bivi, and A. K. Bashir, "Fog-assisted cooperative protocol for traffic message transmission in vehicular networks," *IEEE Access*, vol. 7, pp. 166148–166156, 2019.

[10] H. Zhou, X. Chen, S. He, J. Chen, and J. Wu, "DRAIM: A novel delay-constraint and reverse auction-based incentive mechanism for WiFi offloading," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 4, pp. 711–722, Apr. 2020.

[11] F. Jameel, M. A. Javed, and D. T. Ngo, "Performance analysis of cooperative V2 V and V2I communications under correlated fading," *IEEE Trans. Intell. Transp. Syst.*, early access, Jul. 30, 2019, doi: 10.1109/TITS.2019.2929825.

[12] M. Gonzalez-Martin, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, "Analytical models of the performance of C-V2X mode 4 vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1155–1166, Feb. 2019.

[13] M. A. Javed and E. B. Hamida, "On the interrelation of security, QoS, and safety in cooperative ITS," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 7, pp. 1943–1957, Jul. 2017.

[14] J. Lin, W. Yu, N. Zhang, X. Yang, and L. Ge, "Data integrity attacks against dynamic route guidance in transportation-based cyber-physical systems: Modeling, analysis, and defense," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8738–8753, Sep. 2018.

[15] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.

[16] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2018.

[17] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues," *Future Gener. Comput. Syst.*, vol. 101, pp. 843–864, Dec. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19306909

[18] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3310–3322, Apr. 2020.

[19] F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A comparative analysis of trust models for safety applications in IoT-enabled vehicular networks," in *Proc. Wireless Days (WD)*, Apr. 2019, pp. 1–8.

[20] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[21] M. A. Javed, S. Zeadally, M. Usman, and G. A. S. Sidhu, "FASPM: Fuzzy logic-based adaptive security protocol for multihop data dissemination in intelligent transport systems," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 11, pp. 1–16, 2017.

[22] M. Awais Javed, S. Zeadally, and Z. Hamid, "Trust-based security adaptation mechanism for vehicular sensor networks," *Comput. Netw.*, vol. 137, pp. 27–36, Jun. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861830118X

[23] M. Riveiro, M. Lebram, and M. Elmer, "Anomaly detection for road traffic: A visual analytics framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 8, pp. 2260–2270, Aug. 2017.

[24] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[25] T. T. Dang, H. Y. T. Ngan, and W. Liu, "Distance-based k-nearest neighbors outlier detection method in large-scale traffic data," in *Proc. IEEE Int. Conf. Digit. Signal Process. (DSP)*, Jul. 2015, pp. 507–510.

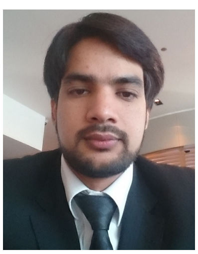
[26] V. Hautamaki, I. Karkkainen, and P. Franti, "Outlier detection using k-nearest neighbour graph," in *Proc. 17th Int. Conf. Pattern Recognit. ICPR*, Aug. 2004, pp. 430–433.

[27] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *Proc. 8th IEEE Int. Conf. Data Mining*, Pisa, Italy, Dec. 2008, pp. 413–422.

MUHAMMAD AWAIS JAVED (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology Lahore, Pakistan, in August 2008, and the Ph.D. degree in electrical engineering from The University of Newcastle, Australia, in February 2015. From July 2015 to June 2016, he was a Postdoctoral Research Scientist with the Qatar Mobility Innovations Center (QMIC) on Safe ITS Project. He is currently an Assistant Professor with COMSATS University Islamabad, Pakistan. His research interests include intelligent transport systems, vehicular networks, protocol design for emerging wireless technologies, and the Internet of Things.

MOHAMMAD ZUBAIR KHAN received the Master of Technology degree in computer science and engineering from U. P. Technical University, Lucknow, India, in 2006, and the Ph.D. degree in computer science and information technology from the Faculty of Engineering, M. J. P. Rohilkhand University, Bareilly, India. He was the Head and an Associate Professor with the Department of Computer Science and Engineering, Invertis University, Bareilly. He has more than 15 years teaching and research experience. He is currently an Associate Professor with the Department of Computer Science, College of Computer Science and Engineering, Taibah University. He has published more than 40 journals and conference papers. His current research interests include data mining, big data, parallel and distributed computing, theory of computations, and computer networks. He has been a member of the Computer Society of India, since 2004.

USMAN ZAFAR received the B.S. and M.S. degrees from COMSATS University Islamabad, in 2017 and 2019, respectively. His research interests include intelligent transport systems, machine learning, and graph theory.



MUHAMMAD FAISAL SIDDIQUI received the B.S. degree in CE and the M.S. degree in EE from the COMSATS Institute of Information Technology, Islamabad, Pakistan, and the Ph.D. degree from the Electrical Engineering Department, Faculty of Engineering, University of Malaya, Kuala Lumpur, Malaysia. He has been an Assistant Professor with the Department of Electrical Engineering, COMSATS University Islamabad, since July 2016. He is currently an Electrical Engineer in digital system design and medical imaging. His research interests include FPGA based digital system designing, bio medical image processing, embedded systems, application speci?c architectural design, and real-time systems.

RABIAH BADAR received the M.S. degree in computer engineering and the Ph.D. degree in electrical engineering from COMSATS University Islamabad, Islamabad, in 2007 and 2009, respectively. From February 2015 to May 2015, she was an Assistant Professor with the Namal College, Mianwali, Pakistan. Since June 2015, she has been an Assistant Professor with COMSATS University Islamabad. She is the author of many international, peer-reviewed journal research articles, conference papers, and book chapters. She has successfully supervised many undergraduate and graduate research thesis. Her research interests include arti?cial intelligence, optimization, soft computing, power system stability and control, nonlinear adaptive control, FACTS, HVDC, and renewable energy systems.

BYUNG MOO LEE (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of California, Irvine, CA, USA, in 2006.

He has ten years of industry experience, including research positions with the Samsung Electronics Seoul Research and Development Center, Samsung Advanced Institute of Technology (SAIT), and Korea Telecom (KT) Research and Development Center. He is currently an Associate Professor with the School of Intelligent Mechatronics Engineering, Sejong University, Seoul, South Korea. He has participated with the IEEE 802.16/11, Wi-Fi Alliance, and 3GPP LTE standardizations. He has also participated in Mobile VCE and Green Touch Research Consortiums, where he made numerous contributions and ?led a number of related patents. His research interests include wireless communications, signal processing, and machine learning applications. He served as the Vice Chairman for the Wi-Fi Alliance Display MTG, from 2015 to 2016.

FARHAN AHMAD (Member, IEEE) received the M.Sc. degree in communication and information technology from the University of Bremen, Germany, in 2014, and the Ph.D. degree in computer science from the College of Engineering and Technology, University of Derby, U.K.. in 2019. He is currently a Postdoctoral Research Fellow with the Cyber Security Research Group, University of Derby. He is also working on the applications of security and trust management in the Industrial IoT (IIoT), e-healthcare, and vehicular ad-hoc networks. His research interests include cyber security and trust management issues in vehicular ad-hoc networks, vehicular cloud networks, M2M communications, smart cities, and the Internet-of-Things (IoT).