# On the Context-Aware Anomaly Detection in Vehicular Networks

Mohammed Abdullatif H. Aljaafari
Department of Management Information Systems-School of Business,
King Faisal University, Alhufof 31982, Saudi Arabia

*Abstract*—**Transportation systems are moving towards autonomous and intelligent vehicles due to advancements in embedded systems, control algorithms, and wireless communications. By enabling connectivity among vehicles, a vehicular network can be developed which offers safe and efficient driving applications. Security is a major challenge for vehicular networks as application reliability depends on it. In this paper, we highlight the security challenges faced by a vehicular network especially related to jamming and data integrity attacks. Such attacks cause major disruptions in the wireless connectivity of users with the centralized servers. We propose a context-aware anomaly detection technique for vehicular networks that considers factors such as signal strength, mobility, and data pattern to find abnormal behaviors and malicious users. We further discuss how an intelligent learning system can be developed using efficient anomaly detection. We implement a vehicular network scenario with malicious users and provide simulation results to highlight the performance gain of the proposed technique. We also highlight several appropriate future opportunities related to the security of vehicular network applications.**

***Keywords*—*Fog computing; load balancing; task offloading***

## I. Introduction

Intelligent Transportation Systems (ITS) are an important component of smart cities. The goal of ITS is to introduce intelligence, connectivity, and control capabilities in the vehicles such that driving can be more safer and comfortable [1]. A vehicular network is an important part of ITS as it provides wireless communication between different components of ITS [2], [3], [4], [5], [6], [7], [8]. The major advantage of vehicular networks is that it can continuously monitor the location of all vehicles within the city and guide the vehicle to make intelligent driving decisions [9], [10], [11]. This can be particularly useful for managing city level traffic flow and accident free driving on the roads [12], [13], [14], [15], [16], [17].

Security and privacy are important aspects of future wireless communications and vehicular networks [18], [19], [20], [21], [22], [23], [24]. Without secure communications, many vehicular network applications can be compromised and sensitive data can be leaked. Thus, security is an important part of reliable communications [25], [26], [27], [28].

Vehicular networks suffer from many attacks by intruders and malicious nodes [29], [30], [31]. These attacks impact the quality of wireless communications, the confidentiality of data transmission, the integrity of messages shared between nodes, and the availability of information among all the devices. By ensuring all these requirements of secure communications, applications' reliability can be significantly improved [9].

Few cyber attacks that target vehicular applications include data integrity attacks, eavesdropping, and jamming. In data integrity attacks, malicious users send wrong information to the server so that data used for making decisions can be polluted [32], [33], [34]. Since most decisions made by the applications rely on the quality of data and its accuracy, it is critical to detect these types of attacks [35], [36], [37].

In eavesdropping attacks, the malicious user captures the data sent between the vehicles and the server [38], [39], [40]. This can be dangerous for applications where sensitive information can be captured and used to impact the vehicle safety [41], [42], [43]. In jamming attacks, malicious users transmit signals to cause interference for other users in the network. This reduces reliability of communications as signal to noise ratio is reduced [44], [45], [46], [47], [48], [49].

To overcome these challenges in the security of vehicular network applications, cryptographic schemes such as Elliptic Curve Digital Signature (ECDSA) are commonly used. By adding extra encryption information to the original message, it is made secure and can only be decoded by users with the correct key information. While ECDSA can make the information and data transmission secure, it is still impacted by cyber-attacks. Particularly, all messages are verified for correct signature information at the receiver. As a result, a lot of time is wasted verifying fake messages by malicious users. This impacts the Quality of Service (QoS) of applications as a large end-to-end delay is incurred.

The data generated by the malicious users can be considered an anomaly or abnormal behavior [50], [51], [52], [53], [54]. The anomalies need to be efficiently detected in a secure system and malicious user data should be recorded for future attack prevention. The goal of anomaly-based security is to complete the process of detection in a quick time and with good accuracy [55], [56], [57], [58].

In this paper, we present a new framework for anomaly detection and verification in vehicular network applications. The key idea of the proposed framework is to develop a trust table in the server for all associated vehicular nodes in the network. The framework uses contextual information related to message physical parameters, mobility of the user, and data patterns to compute trust and detect anomalies. Moreover, the framework also includes an anomaly verification procedure so that the trust values in the trust table can be updated periodically on the server. Simulation results in MATLAB provide a detailed performance evaluation of the proposed technique compared to the other recent techniques in the literature. Finally, we also present several research challenges and future opportunities in the area of vehicular network security.

Table I below shows the anomaly detection techniques in the literature.

## II. Literature Review

Security and privacy in vehicular and IoT systems have been explored in several papers in the literature. Similarly, anomaly detection techniques have been part of many proposals. We discuss some of these techniques in this section.

The work in [59] proposes a novel anomaly detection technique for IoT networks. The major problem addressed in this paper is related to class imbalance i.e. when normal data is much larger than the abnormal one or vice versa. The data set considered in this paper is Network Security Laboratory-Knowledge Discovery and Data Mining Tools Competition (NSL-KDD). The technique used in this paper is reinforcement learning in which actions are classification of input data into normal and malicious categories. The states in the paper are the data type. As the data in an IoT network can be of different types. Hence, the state takes into account the data category. The reward function in the paper is anomaly prediction accuracy. The proposed work shows better accuracy, recall, and F1 score.

In [60], the authors focus on a network related to Industrial IoT (IIoT). The goal is to detect cyber attacks and a federated learning-based approach is used in this regard. The major advantage of the federated learning approach is its privacy preservation as data is only shared locally. In the proposed work, universal anomaly detection is achieved with the help of different local Anomaly Detection Centers (ADC). Moreover, anomalous ADCs are also detected with the proposed technique. There is also an appeal procedure reserved for users that are declared anomalous. The accuracy and throughput of the proposed technique are shown to be better than other related techniques.

The work in [61] deals with traffic flow monitoring applications for Software Defined Networks (SDN). The goal of the technique is to choose traffic flow monitoring granularity. There exists a tradeoff between accuracy and network load. More accurate techniques may incur a large network load, hence a balancing technique is needed. The proposed technique uses Deep-Q learning to detect anomalies. The proposed technique achieves quick and optimal policy evaluation. Particularly against the Denial of Service (DDoS) attacks, the proposed technique performs efficiently. The accuracy and detection time of the proposed technique has been shown to perform better than other techniques in the literature.

In [56], the authors considered an Internet of Vehicles (IoV) scenario where vehicles share information about the surrounding traffic. Parameters such as traffic density, vehicles in an emergency, vehicle speeds, etc. are shared with infrastructure Road Side Units (RSUs). Malicious users launch data integrity attacks i.e., they change the information about traffic density and send wrong information. As a result, the traffic density estimation is corrupted and wrong decisions are made. To overcome this problem, the authors propose an isolation forest-based anomaly detection algorithm. The anomalies are verified using probe messages that are sent to vehicles in the neighborhood of malicious users. A communication mechanism is also designed to share the verification information. Results in terms of accuracy, recall, and F1 score of the proposed technique is enhanced.

The social networks are considered as part of the work in [62]. The main problem addressed is related to feature learning and combining information from the neighborhood. Based on feature gathering, Graph Neural Network (GNN) technique is proposed that uses GNN based encoder for feature learning. For efficient training, pattern mining algorithms are used by the proposed technique. A novel loss function is also proposed in the work. Metrics such as precision, recall, and F1 score are shown to be improved as compared to other techniques.

The work in [63] deals with improving the security of the Domain Name System (DNS). The key idea used is to make the system topology aware and consider the structural properties of the network. The technique used is the exponential random graph model and the topology is converted into the graph format. A time series analysis is also applied for anomaly detection. The autoregressive moving average is used for the time series analysis. The precision and recall of the system are improved as compared with other techniques.

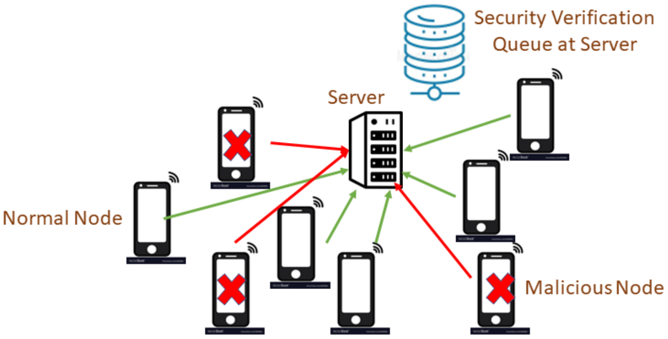

Fig. 1. Considered system model.

## III. System Model

In this paper, we consider a wireless transmission scenario where several vehicular nodes are sharing their data with a centralized server or Road Side Unit (RSU) as shown in Fig. 1. This data can be traffic mobility information, tasks for offloading, service query requests, etc. The server authenticates each vehicular user using traditional cryptographic mechanisms. Moreover, vehicular users also share their messages using digital signature schemes.

Several malicious vehicle nodes are also present in the vicinity of the normal vehicle nodes and servers. These users can carry out several types of attacks such as jamming signal transmissions, eavesdropping, data integrity attacks, etc. These attacks can significantly disrupt the data security and reliability of the wireless system.

The server receives messages from both normal vehicle users and malicious vehicle users. These messages are placed in a queue and a digital signature verification algorithm is applied to messages one by one. The messages from malicious users result in additional queuing delays at the server. Some messages may be discovered to be malicious after the signature

TABLE I. Anomaly Detection Techniques in the Literature

| Network | Main Idea | Technique Used | Results |
|---|---|---|---|
| IoT [59] | Anomaly Detection<br>Class imbalance problem<br>NSL-KDD data set | Reinforcement Learning<br>Action - Classify input data<br>State - Data type<br>Reward - Prediction accuracy | Accuracy<br>Recall<br>F1 score |
| IIoT [60] | Detect cyber attacks<br>Federated learning<br>Privacy preservation | Universal anomaly detection<br>Anomalous ADC detection<br>Appeal procedure for users | Accuracy<br>Throughput |
| SDN [61] | Traffic flow monitoring<br>Monitoring granularity<br>Accuracy vs network load | Deep Q leaning<br>Quick optimal policy evaluation<br>DDoS attack detection | Accuracy<br>Detection time |
| IoV [56] | Data Integrity attacks<br>Traffic density information<br>Information checking | Isolation Forest<br>Verify anomalies<br>Neighborhood verification | Accuracy<br>Recall<br>F1 score |
| Social networks [62] | Feature learning<br>Combine neighborhood information | Graph Neural Network (GNN)<br>GNN encoder for feature learning<br>Pattern mining algorithms for training<br>Novel loss function | Precision<br>Recall<br>F1 score |
| DNS [63] | Topology aware<br>Structural properties of network | Exponential Random Graph Model<br>Time series analysis<br>Auto regressive moving average | Precision<br>Recall |

verification, but the time spent in their verification causes an extra delay for the messages.

In addition, some malicious messages have the correct digital signature but are launched to disrupt the wireless transmissions. These messages pass through the digital signature verification stage but impact the system latency. Without an efficient anomaly detection technique, these messages can not be detected on the run. Even their malicious behavior is not learned due to the absence of an anomaly detection mechanism and can not be detected in the future.

## IV. Proposed Anomaly Detection Framework

The proposed anomaly detection framework is shown in Fig. 2. The server maintains an anomaly detection module in its storage. The anomaly detection module consists of several blocks which are explained in the following subsections. The goal of the proposed framework is to shortlist and sideline anomalies so that server does not waste time in signature verification of malicious user messages.

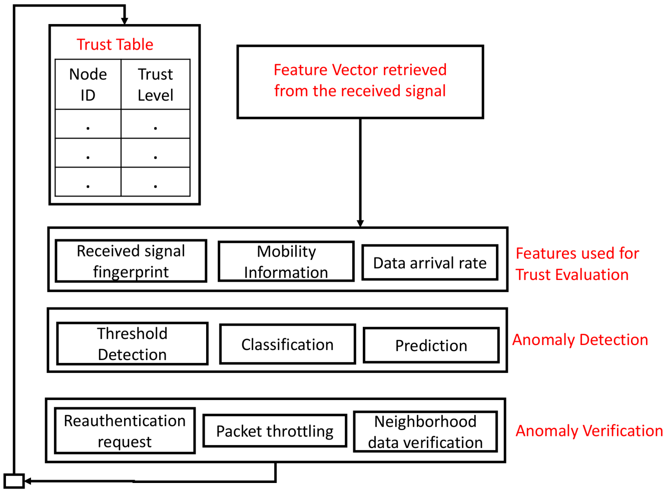

Fig. 2. Proposed context-aware anomaly detection framework.

### *A. Trust Table*

Each server maintains a trust table that contains trust levels computed for each vehicle in the network. The trust table is a lookup table that contains two columns and several rows. The columns include information about node ID and trust level. The rows are equal to the number of vehicles in the network of the server.

A new vehicle that is entered in the coverage range of the server is registered in the trust table once it starts sharing its data with the server. Based on the data received from the vehicle nodes, the trust table is updated on regular basis i.e., the trust values are updated.

A timer value is used by the server to keep a check on the current status of the vehicle nodes in the network. Vehicles that do not send data for a long time are removed from the trust table. The reason for this is that either the vehicles have moved out of the coverage range of the server or the device has been turned off. As a result, the trust look-up table is shortened by the removal of such devices. This reduces the search time for a device's trust from the look-up table.

Trust table is evaluated based on fuzzy logic as shown in Table II. We explain the features used for developing the trust table in the next subsections.

TABLE II. TRUST EVALUATION BASED ON FUZZY LOGIC

| **Trust Feature** | **Trust Value Threshold** | | |
|---|---|---|---|
| | **Low** | **Medium** | **High** |
| **Received Signal Fingerprint ($F_{inc}$)** | $\geq 0.6$ | 0.3-0.6 | 0-0.3 |
| **Mobility Information ($T_r^{inc}$)** | 0-100 ms | 100 ms-500 ms | 500 ms-1 s |
| **Data Arrival Rate ($D_A$)** | $\geq 20p/s$ | 10-20 p/s | 0-10 p/s |

### *B. Trust Evaluation*

Trust evaluation is the most critical block of the anomaly detection module. Trust in our proposal is computed based on several features considering the general behavior of malicious vehicles. The proposal is context-aware in the sense that the environment, data transmission, and mobility factors related to vehicular network are considered while evaluating trust.

The trust evaluation in our proposal is based on both the historic long-term data of the used features as well as the current feature vector. An average value of the features used in our proposal is maintained by the server. The advantage of storing long-term data is to evaluate the trend of the features and efficiently detect anomalies.

The following vehicle features are used for the trust evaluation in the proposed framework. The evaluation mechanism of each feature and its rationale are presented below. It is to be noted that these are physical features that are obtained using the obtained signal. These features are selected before the signature verification mechanism so that malicious messages are not verified.

*1) Received signal-based fingerprint:* The received signal can provide useful identification of devices in the network. In this regard, Signal Interference and Noise Ratio (SINR) and Angle of Arrival (AoA) retrieved from the signal can act as a fingerprint for a device. The received power from a device can be calculated as follows:

$$P_r = G_c \frac{P_t}{d^\gamma} \tag{1}$$

Here $P_r$ is the received power, $G_c$ is the channel gain, $P_t$ is the transmitted power, $d$ is the distance between the transmitter and the receiver, and $\gamma$ is the path loss index. The value of the path loss index can vary between $2$ and $4$ depending on the scenario. The channel gain also varies depending on the channel conditions. In many scenarios, multi-path fading introduces varying channel gains depending on the amount of reflection and refraction from different objects.

The SINR at the server can be computed from the following equation:

$$SINR = \frac{P_r}{I + N_O} \tag{2}$$

where

$$I = \sum_{v=1}^{M} P_{r,v} \tag{3}$$

From Eq. (2), SINR is evaluated from the ratio of received power $P_r$ and total noise in the system. There are two components of total noise. One is the background noise $N_O$ and the other is the total interference. If the server receives $v$ signals at the same time, the total interference can be computed from Eq.( 3). This is the summation of all signals transmitted from those $v$ vehicles.

Using the received signal, a map between physical location and user is developed. Any malicious user that is sending wrong location information to launch jamming attacks may be identified. The fingerprint can also be used to find areas that are critical concerning security and have more density of malicious users.

As shown in Table II, we map the received signal finger print value to the trust value using three categories; low, medium and high. The server tracks the fingerprint value of each vehicle based on its current location as follows:

$$F = \frac{SINR}{d} \tag{4}$$

The incremental change in fingerprint $F_{inc}$ is given as

$$F_{inc} = \frac{|F_{new} - F_{old}|}{F_{old}} \tag{5}$$

If $F_{inc}$ is greater than 0.6, the corresponding trust value can be mapped to a low value. Similarly, a medium trust value means a $F_{inc}$ value between 0.3 and 0.6. Lastly, a high trust value means a low $F_{inc}$ value of less than 0.3. The rationale behind this approach is that malicious vehicles will be sending either wrong location information in its message or using high transmit power from its correct location for the attack. This factor is captures in the metric $F_{inc}$.

*2) Mobility information:* Mobility is an important parameter that can provide useful information about the normal behavior of nodes. Malicious users may periodically change their position to transmit their information so that they are off the radar. As a result, the percentage change in location of nodes is determined and those devices whose position is changing randomly in an abnormal manner is shortlisted for anomaly evaluation.

Since mobility information can only be obtained once the message is verified and decoded, it is not possible to get this information at the physical level. To overcome this problem, signal power is used as an estimate of the position of the sender. In literature, some techniques can estimate the location of the sender using received signal power [64]. The sender location is estimated in the form of distance bins rather than the exact longitude and latitude.

The distance bin of the initial location of the sender is noted based on the last message sent to the server. The node ID of the sender is noted down once the signature of the message is verified. A local map for node ID and its distance bin is stored in the server. Once, the same node changes its location and distance bin by a certain threshold for the next message, the node is marked as a possible malicious node and short-listed for the verification phase.

In Table II we use time to reach from vehicle to server ($T_r$) as the metric to evaluate change in sudden location of the vehicle. $T_r$ is evaluated as follows:

$$T_r = \frac{d}{speed} \tag{6}$$

The incremental change in $T_r^{inc}$ is given as

$$T_r^{inc} = |\frac{T_r^{new} - T_r^{old}|}{T_r^{old}} \tag{7}$$

A low trust value refers to a high $T_r^{inc}$ which means either the speed of the vehicle or the location of the vehicle obtained from the received message is suddenly changed.

*3) Data arrival rate:* The data arrival rate can also provide information about the possible malicious behavior of a node. Malicious users may try to jam the network by sending repeated requests for task computation or sending incorrect data messages as part of data integrity attacks. The data inter-arrival rate for a particular node is computed as the difference between the time when the current message is received and the time when the last message was sent. This time is computed once the messages are verified for digital signature correction.

To overcome this problem, the inter-arrival time between two messages is checked regularly. Once a certain arrival rate is crossed, those nodes is marked as malicious for checking. Besides data arrival rate, message size can also be checked as malicious users may transmit large packets to negatively impact the bandwidth usage and increase the signature verification time.

*4) Data variation:* The data variation is a critical metric that can be used to detect anomalies specifically in the cases of malicious users that are sending wrong unrelated information. An example of this data integrity attack could be a traffic management application where wrong traffic density values are shared with the server. As a result, data variation sent from sensors located in a geographical location should raise alarms and should be checked for anomalies. In Table II, we utilize a data arrival rate of greater than 20 packets per second (p/s) to be marked as a value with low trust. This is because generally, the packet frequency of vehicular network varies from 1 to 10 packets/second. Hence, we give a higher trust value to nodes which conform with this requirement and send packets within the allowed range of 1-10 packets per second.

### *C. Anomaly Detection*

In this phase, nodes that are marked as anomalous or malicious are noted down and a list is maintained. This list includes all the nodes that are on the radar for anomaly detection and a further investigation of their status is needed. For maintaining this list, techniques such as threshold detection, cumulative distribution function evaluation, standard deviation, etc. is applied to the features data from the previous block.

There exists a trade-off between the accuracy of anomaly detection and the time for evaluating the anomaly. If the threshold is kept too strict, only a few users may be marked as anomalous and anomaly verification is done quickly. However, many malicious nodes may be missed. On the other hand, if the threshold is kept too loose, many users will be short-listed for anomaly verification. This will need more message overhead and time needed to verify each anomaly. As a result, extra bandwidth and time will be needed.

In this work, we utilize fuzzy logic to evaluate anomalies. We first calculate trust levels based on individual features as described in Table II. Finally, we utilize majority voting to find the overall trust level. This means that the trust level is categorized as high if the trust based on at least two of the features are evaluated as high. Data from all nodes which have a low and medium trust levels are marked as anomalous.

### *D. Anomaly Verification*

In this block, the shortlisted malicious users is tracked for further verification so that actual anomalies are picked up. For this, short-listed users send a message to inform them about their entry into the malicious node list. Those nodes may need to re-authenticate themselves before sending any further messages. All those nodes that can re-authenticate are allowed to start transmitting their messages again.

Another way to verify anomalies used in the proposed technique is packet throttling requests. The users are asked to reduce their data rates. All users that follow this request are allowed to continue sending messages. However, those nodes that do not follow the instructions and keep on sending a large number of messages which are marked as malicious users who are launching jamming attacks.

One technique to verify anomalies is neighborhood verification. This is particularly useful for data integrity attacks. The area of those nodes that are sending wrong information and marked as possible malicious nodes are noted down. The list of neighboring nodes are sent probe messages to find if the information sent by malicious nodes is correct or not. This technique however is suited for those applications in which the sensed information in the neighborhood is nearly the same, for example, temperature monitoring in an area, average vehicle traffic density on a road segment, etc.

TABLE III. Simulation Parameters

| **Simulation Parameter** | **Value** |
|---|---|
| Number of vehicular nodes | 200 |
| Packet Generation Rate | 10 per second |
| Number of Malicious users | 50-200 |
| Security Algorithm | ECDSA |
| Hash Function Used | SHA-256 |
| Message size | 7400 bits |
| Security overhead | 1600 bits |
| Total Packet Size | 9000 bits |
| Security Verification Time | 0.5ms |
| Packet expiry time | 3ms |

## V. Performance Evaluation

In this section, the performance evaluation of the Proposed Technique (PT) is presented. The results are compared with two other techniques. The first one is the Outlier Detection, Prioritization, and Verification (ODPV) algorithm which uses an isolation forest algorithm to detect anomalies. The second algorithm is the K-Nearest Neighbor (KNN) algorithm which uses majority voting to make decisions about the anomaly.

### *A. Simulation Model*

The simulation model is developed in MATLAB and its parameters are given in Table III. The number of vehicular nodes is taken as 200. The packet generation rate of each vehicular node is 10 packets per second. The number of malicious users is 50-200. The malicious users also generate packets at the same rate as the malicious users with wrong information about the sensing parameters and causing data integrity attacks. Also, the malicious users continuously change their positions. As a result, received signal strength, mobility, and data variation factors come into play.

The security algorithm used is the Elliptic Curve Digital Signature (ECDSA) algorithm and the hash function used is the Secure Hashing Algorithm (SHA) with a key size of 256 bits. The message size generated by vehicular devices is 7400 bits and the security overhead for the ECDSA algorithm is 1600 bits [9]. The total packet size is 9000 bits. The security verification time for each packet is 0.5ms. The packet expiry time is 3ms.

### *B. Results*

For results, we take the following four metrics defined as follows:

*1) Security verification time:* This is the time needed to verify the digital signature as per the ECDSA algorithm. The security verification time depends on the key bit size used by the ECDSA algorithm. Moreover, the security verification time increases with the number of messages.

*2) Total delay:* The delay is the sum of the transmission time and security verification time. The transmission time depends on the message size and data rate.

*3) Percentage of packets expired:* The percentage of packets expired includes the percentage of packets that could not be verified within the time limit of 3ms.

*4) Shortlisted packets and anomaly packets:* The shortlisted packets include the number of packets that were originally shortlisted by the anomaly detection technique. The anomaly packets are the number of packets that were declared as anomaly after verification.

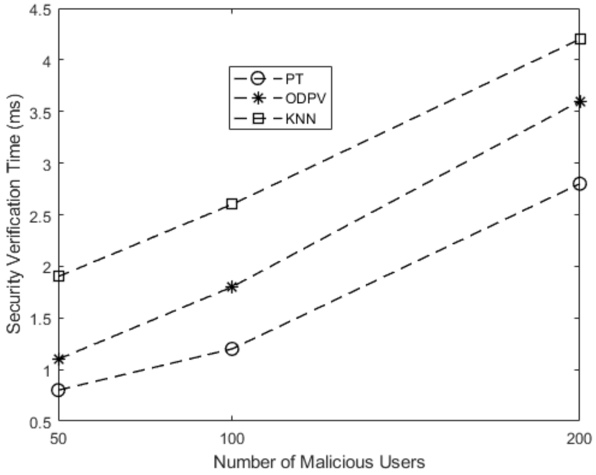

Fig. 3. Security verification time vs Number of malicious users.

Fig. 3 shows the security verification time of packets as the number of malicious users is increased from 50 to 200. The results show that the security verification time of the proposed technique is up to 1ms better than the other two techniques namely, ODPV and KNN. This is due to using context-aware parameters for trust evaluation and anomaly detection. As a result, the anomaly packets are identified after the first few iterations, and the overall network load on the server is reduced. This results in reduced security verification time.

In Fig. 4, the plot of malicious users vs total delay is shown for the three algorithms. The proposed technique has the least delay in packet transmission and hence, is very useful for vehicular applications. As compared to ODPV and KNN, the delay values of the proposed technique show up to 50% reduction. As the number of malicious users increased up to 200, the results of the proposed technique are much better than the other two techniques.

Fig. 5 shows the results of the percentage of packets expired for the three algorithms. The proposed technique has excellent results with only less than 10% packet expiry rate

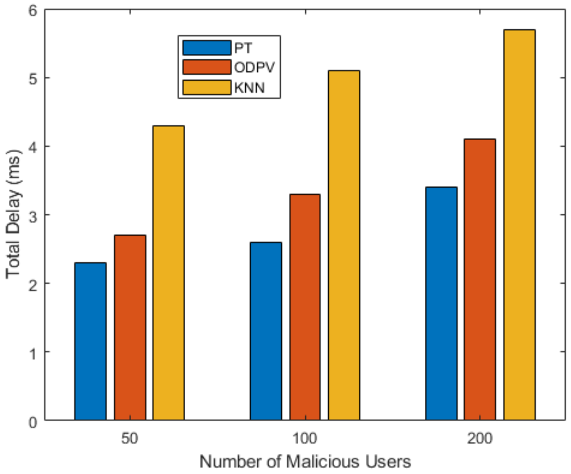

Fig. 4. Total delay vs Number of malicious users.

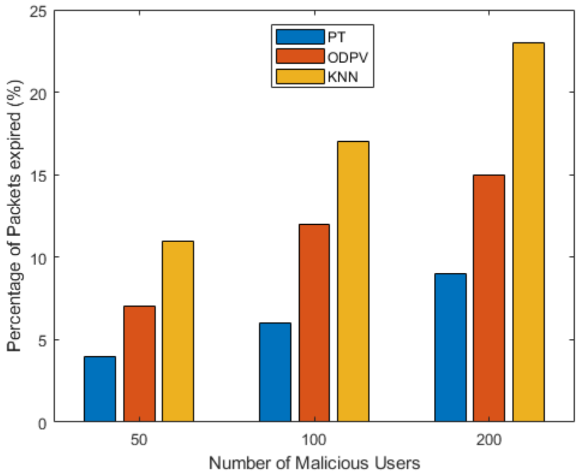

Fig. 5. Percentage of packets expired vs Number of malicious users.

as compared to the ODPV and KNN that has up to 15% and 22% packets expiry rate.

Lastly, Fig. 6 shows the anomaly detection accuracy performance of the proposed technique. The proposed technique almost accurately shortlists the packets which are anomalous when the number of malicious users is 50. As the malicious users increased, the difference between shortlisted packets and anomaly packets increased. This is because, at a lower number of nodes, the anomalous packets are easier to detect after a few iterations. As the number of packets is increased, less number of packets meet all the context-related conditions and hence fall into the likely malicious category. However, after verification, the anomaly packets out of the shortlisted ones are picked up by the algorithm.

## VI. Future Opportunities

In this section, future opportunities are provided related to the challenges in the security of vehicular applications.

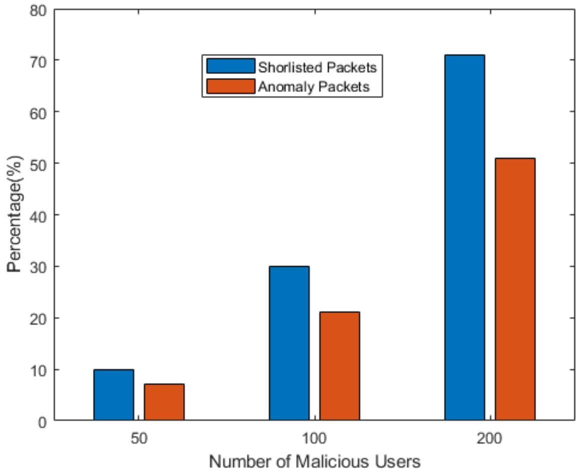

Fig. 6. Shortlisted packets vs Anomaly packets by the proposed technique.

### A. Learning based Algorithms

Machine learning-based algorithms can be designed to adaptively vary the trust levels using context-aware data from different vehicular devices. Appropriate neural networks can be developed to predict the users which are malicious or geographical areas where malicious users reside. Moreover, reinforcement learning algorithms can also be useful for optimal security-related policy design such as priority-based security verification of incoming messages. Similarly, anomaly detection can also be improved using classification algorithms based on data of malicious and normal users. Related with the current work, a learning algorithm can be used to find the appropriate threshold for anomaly detection based on incremental changes in the fingerprint, location and speed values of the vehicles.

### B. Graph based Algorithms

Graph theory algorithms are very useful for evaluating the trust of vehicular devices. For example, metrics such as centrality and degree of nodes can be taken into account when evaluating the trust. Stable matching algorithms can also be used for sending authentication requests by vehicular devices to appropriate servers depending on factors such as data rate, and load on the servers. Similarly, breadth-first search and depth-first search algorithms can be used for searching anomalies from the data sets, and also for finding an efficient route for reaching the nodes for data verification. Graph theory algorithms can also be used to verify anomalies from vehicles with high centrality values or vehicles with highest trust values. This will improve the accuracy of the verification process.

### C. Blockchain Techniques

Besides, trust-based anomaly detection techniques, blockchain security mechanisms can also be used to enhance the privacy of data sharing. With blockchain, smaller key sizes of the ECDSA algorithm can be used as added security will be provided with blockchain. However, a major challenge in designing such techniques will be the delay in mining the blockchain nodes and appropriate consensus algorithms. The proposed work of anomaly detection can also be used to find malicious mining nodes which can disrupt the security of blockchain. Moreover, new context-aware algorithms considering different features can be designed for the particular blockchain mining application.

## VII. Conclusion

In this paper, we present an overview of anomaly detection for vehicular applications. We discuss recent work in the literature related to anomaly detection. We present a novel framework for anomaly detection which uses context-related information such as physical signal parameters to classify anomalies without security verification. The proposed technique also includes an anomaly verification phase and develops a trust table for each node in the network. Finally, we highlight several important research directions in the area of security of vehicular and anomaly detection.

## References

[1] M. A. Javed, T. N. Nguyen, J. Mirza, J. Ahmed, and B. Ali, "Reliable communications for cybertwin driven 6g iovs using intelligent reflecting surfaces," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2022.

[2] G. Xie, K. Yang, C. Xu, R. Li, and S. Hu, "Digital twinning based adaptive development environment for automotive cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1387–1396, 2022.

[3] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784–800, 2022.

[4] X. Zhang, H. Ma, and C. K. Tse, "Assessing the robustness of cyber-physical power systems by considering wide-area protection functions," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 12, no. 1, pp. 107–114, 2022.

[5] X. Ning and J. Jiang, "Design, analysis and implementation of a security assessment/enhancement platform for cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1154–1164, 2022.

[6] M. Hussain, N. Ali, and J.-E. Hong, "Deepguard: a framework for safeguarding autonomous driving systems from inconsistent behaviour," *Automated Software Engineering*, vol. 29, no. 1, p. 1, 2022.

[7] J. Valinejad, L. Mili, C. N. van der Wal, and Y. Xu, "Environomic-based social demand response in cyber-physical-social power systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 1302–1306, 2022.

[8] S. V. Thiruloga, V. K. Kukkala, and S. Pasricha, "Tenet: Temporal cnn with attention for anomaly detection in automotive cyber-physical systems," in *2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2022, pp. 326–331.

[9] M. A. Javed, E. B. Hamida, and W. Znaidi, "Security in intelligent transport systems for smart cities: From theory to practice." *Sensors*, vol. 16, no. 6, p. 879, July 2016.

[10] D. Zhao, C. Liu, G. Xu, Z. Ding, H. Peng, J. Yu, and J. Han, "A security enhancement model based on switching edge strategy in interdependent heterogeneous cyber-physical systems," *China Communications*, vol. 19, no. 2, pp. 158–173, 2022.

[11] D. Cheng, J. Shang, and T. Chen, "Finite-horizon strictly stealthy deterministic attacks on cyber-physical systems," *IEEE Control Systems Letters*, vol. 6, pp. 1640–1645, 2022.

[12] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377–391, 2022.

[13] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1282–1291, 2022.

[14] G. Sun, T. Alpcan, B. I. P. Rubinstein, and S. Camtepe, "Securing cyber-physical systems: Physics-enhanced adversarial learning for autonomous platoons," in *Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2022, Grenoble, France, September 19–23, 2022, Proceedings, Part III*. Berlin, Heidelberg: Springer-Verlag, 2023, p. 269–285.

[15] C. Qian, X. Liu, C. Ripley, M. Qian, F. Liang, and W. Yu, "Digital twin-cyber replica of physical things: Architecture, applications and future research directions," *Future Internet*, vol. 14, no. 2, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/2/64

[16] R. Müller, F. Kessler, D. W. Humphrey, and J. Rahm, "Data in context: How digital transformation can support human reasoning in cyber-physical production systems," *Future Internet*, vol. 13, no. 6, 2021. [Online]. Available: https://www.mdpi.com/1999-5903/13/6/156

[17] M. Hussain and J.-E. Hong, "Enforcing safety in cooperative perception of autonomous driving systems through logistic chaos map-based end-to-end encryption," in *2022 16th International Conference on Open Source Systems and Technologies (ICOSST)*, 2022, pp. 1–6.

[18] G. Li, C. Lai, R. Lu, and D. Zheng, "Seccdv: A security reference architecture for cybertwin-driven 6g v2x," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 4535–4550, 2022.

[19] M. A. Javed and E. B. Hamida, "On the interrelation of security, qos, and safety in cooperative its," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 7, pp. 1943–1957, July 2017.

[20] S. Soderi and R. De Nicola, "6g networks physical layer security using rgb visible light communications," *IEEE Access*, vol. 10, pp. 5482–5496, 2022.

[21] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6g," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 53–87, 2022.

[22] M. A. Javed, S. Zeadally, and Z. Hamid, "Trust-based security adaptation mechanism for vehicular sensor networks," *Computer Networks*, vol. 137, pp. 27 – 36, 2018.

[23] D. P. Moya Osorio, I. Ahmad, J. D. V. Sánchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, "Towards 6g-enabled internet of vehicles: Security and privacy," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 82–105, 2022.

[24] M. Hussain, N. Ali, and J.-E. Hong, "Vision beyond the field-of-view: A collaborative perception system to improve safety of intelligent cyber-physical systems," *Sensors*, vol. 22, no. 17, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/17/6610

[25] S. A. Soleymani, S. Goudarzi, M. H. Anisi, Z. Movahedi, A. Jindal, and N. Kama, "Pacman: Privacy-preserving authentication scheme for managing cybertwin-based 6g networking," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4902–4911, 2022.

[26] H. Cao, J. Du, H. Zhao, D. X. Luo, N. Kumar, L. Yang, and F. R. Yu, "Toward tailored resource allocation of slices in 6g networks with softwarization and virtualization," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6623–6637, 2022.

[27] M. A. Javed, E. B. Hamida, A. Al-Fuqaha, and B. Bhargava, "Adaptive security for intelligent transport system applications," *IEEE Intelligent Transportation Systems Magazine*, vol. 10, no. 2, pp. 110–120, 2018.

[28] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. P. C. Rodrigues, "An anonymous batch authentication and key exchange protocols for 6g enabled vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1630–1638, 2022.

[29] T.-V. Le, C.-F. Lu, C.-L. Hsu, T. K. Do, Y.-F. Chou, and W.-C. Wei, "A novel three-factor authentication protocol for multiple service providers in 6g-aided intelligent healthcare systems," *IEEE Access*, vol. 10, pp. 28 975–28 990, 2022.

[30] N. Fotiou, V. A. Siris, G. Xylomenos, and G. C. Polyzos, "Iot group membership management using decentralized identifiers and verifiable credentials," *Future Internet*, vol. 14, no. 6, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/6/173

[31] D. Marabissi, L. Mucchi, and A. Stomaci, "Iot nodes authentication and id spoofing detection based on joint use of physical layer security and machine learning," *Future Internet*, vol. 14, no. 2, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/2/61

[32] D. An, F. Zhang, Q. Yang, and C. Zhang, "Data integrity attack in dynamic state estimation of smart grid: Attack model and countermeasures," *IEEE Transactions on Automation Science and Engineering*, pp. 1–14, 2022.

[33] H. Yu, Q. Hu, Z. Yang, and H. Liu, "Efficient continuous big data integrity checking for decentralized storage," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1658–1673, 2021.

[34] H. Wu, B. Zhou, and C. Zhang, "Secure distributed estimation against data integrity attacks in internet-of-things systems," *IEEE Transactions on Automation Science and Engineering*, pp. 1–14, 2021.

[35] Y. Zhao, X. Gong, F. Lin, and X. Chen, "Data poisoning attacks and defenses in dynamic crowdsourcing with online data quality learning," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[36] T. Hong and A. Hofmann, "Data integrity attacks against outage management systems," *IEEE Transactions on Engineering Management*, vol. 69, no. 3, pp. 765–772, 2022.

[37] Y. Luo, L. Cheng, Y. Liang, J. Fu, and G. Peng, "Deepnoise: Learning sensor and process noise to detect data integrity attacks in cps," *China Communications*, vol. 18, no. 9, pp. 192–209, 2021.

[38] X. Zhong, C. Fan, and S. Zhou, "Eavesdropping area for evaluating the security of wireless communications," *China Communications*, vol. 19, no. 3, pp. 145–157, 2022.

[39] ——, "Eavesdropping area for evaluating the security of wireless communications," *China Communications*, vol. 19, no. 3, pp. 145–157, 2022.

[40] B. Li, Y. Yao, H. Zhang, Y. Lv, and W. Zhao, "Energy efficiency of proactive eavesdropping for multiple links wireless system," *IEEE Access*, vol. 6, pp. 26 081–26 090, 2018.

[41] B. Li, Y. Yao, H. Zhang, and Y. Lv, "Energy efficiency of proactive cooperative eavesdropping over multiple suspicious communication links," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 420–430, 2019.

[42] G. Savva, K. Manousakis, and G. Ellinas, "Eavesdropping-aware routing and spectrum/code allocation in ofdm-based eons using spread spectrum techniques," *Journal of Optical Communications and Networking*, vol. 11, no. 7, pp. 409–421, 2019.

[43] J. Moon, S. H. Lee, H. Lee, and I. Lee, "Proactive eavesdropping with jamming and eavesdropping mode selection," *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3726–3738, 2019.

[44] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[45] S. Hu, D. Yue, C. Dou, X. Xie, Y. Ma, and L. Ding, "Attack-resilient event-triggered fuzzy interval type-2 filter design for networked nonlinear systems under sporadic denial-of-service jamming attacks," *IEEE Transactions on Fuzzy Systems*, vol. 30, no. 1, pp. 190–204, 2022.

[46] J. Liu, X. Wang, S. Shen, Z. Fang, S. Yu, G. Yue, and M. Li, "Intelligent jamming defense using dnn stackelberg game in sensor edge cloud," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4356–4370, 2022.

[47] L. Zhao, H. Xu, J. Zhang, and H. Yang, "Resilient control for wireless cyber-physical systems subject to jamming attacks: A cross-layer dynamic game approach," *IEEE Transactions on Cybernetics*, vol. 52, no. 4, pp. 2599–2608, 2022.

[48] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Effects of jamming attacks on wireless networked control systems under disturbance," *IEEE Transactions on Automatic Control*, pp. 1–1, 2022.

[49] J. Villain, V. Deniau, C. Gransart, A. Fleury, and E. P. Simon, "Characterization of ieee 802.11 communications and detection of low-power jamming attacks in noncontrolled environment based on a clustering study," *IEEE Systems Journal*, vol. 16, no. 1, pp. 683–692, 2022.

[50] C. Zhang, W. Zuo, P. Yang, Y. Li, and X. Wang, "Outsourced privacy-preserving anomaly detection in time series of multi-party," *China Communications*, vol. 19, no. 2, pp. 201–213, 2022.

[51] C. Huang, Z. Yang, J. Wen, Y. Xu, Q. Jiang, J. Yang, and Y. Wang, "Self-supervision-augmented deep autoencoder for unsupervised visual anomaly detection," *IEEE Transactions on Cybernetics*, pp. 1–14, 2021.

[52] C. Huang, J. Wen, Y. Xu, Q. Jiang, J. Yang, Y. Wang, and D. Zhang, "Self-supervised attentive generative adversarial networks for video anomaly detection," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–15, 2022.

[53] W. A. Yousef, I. Traoré, and W. Briguglio, "Un-avoids: Unsupervised and nonparametric approach for visualizing outliers and invariant detection scoring," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5195–5210, 2021.

[54] X. Ma, J. Wu, S. Xue, J. Yang, C. Zhou, Q. Z. Sheng, H. Xiong, and L. Akoglu, "A comprehensive survey on graph anomaly detection with deep learning," *IEEE Transactions on Knowledge and Data Engineering*, pp. 1–1, 2021.

[55] W. Wang, Z. Wang, Z. Zhou, H. Deng, W. Zhao, C. Wang, and Y. Guo, "Anomaly detection of industrial control systems based on transfer learning," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 821–832, 2021.

[56] M. A. Javed, M. Z. Khan, U. Zafar, M. F. Siddiqui, R. Badar, B. M. Lee, and F. Ahmad, "Odpv: An efficient protocol to mitigate data integrity attacks in intelligent transport systems," *IEEE Access*, vol. 8, pp. 114 733–114 740, 2020.

[57] W. Wang, W. Song, Z. Li, B. Zhao, and B. Zhao, "A novel filter-based anomaly detection framework for hyperspectral imagery," *IEEE Access*, vol. 9, pp. 124 033–124 043, 2021.

[58] Y.-H. Nho, S. Ryu, and D.-S. Kwon, "Ui-gan: Generative adversarial network-based anomaly detection using user initial information for wearable devices," *IEEE Sensors Journal*, vol. 21, no. 8, pp. 9949–9958, 2021.

[59] X. Ma and W. Shi, "Aesmote: Adversarial reinforcement learning with smote for anomaly detection," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 943–956, 2021.

[60] X. Wang, S. Garg, H. Lin, J. Hu, G. Kaddoum, M. Jalil Piran, and M. S. Hossain, "Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7110–7119, 2022.

[61] T. V. Phan, T. G. Nguyen, N.-N. Dao, T. T. Huong, N. H. Thanh, and T. Bauschert, "Deepguard: Efficient anomaly detection in sdn with fine-grained traffic flow monitoring," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1349–1362, 2020.

[62] T. Zhao, T. Jiang, N. Shah, and M. Jiang, "A synergistic approach for graph anomaly detection with pattern mining and feature learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 6, pp. 2393–2405, 2022.

[63] M. Tsikerdekis, S. Waldron, and A. Emanuelson, "Network anomaly detection using exponential random graph models and autoregressive moving average," *IEEE Access*, vol. 9, pp. 134 530–134 542, 2021.

[64] E. B. Hamida and M. A. Javed, "Channel-aware ECDSA signature verification of basic safety messages with k-means clustering in VANETs," in *Proc. IEEE Intl. Conf. on Advanced Information Networking and Applications*, 2016, pp. 1–8.