Alexandria Engineering Journal 78 (2023) 131–140

Contents lists available at ScienceDirect

Alexandria Engineering Journal

journal homepage: www.elsevier.com/locate/aej

Original Article

A secure and trusted context prediction for next generation autonomous vehicles☆

Geetanjali Rathee [a], Sahil Garg [b,*], Georges Kaddoum [c,d], Bong Jun Choi [e], Abderrahim Benslimane [f], Mohammad Mehedi Hassan [g]

[a] Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi, India
[b] Electrical Engineering Department, École de technologie supérieure, Université du Québec, Montréal, QC H3C 1K3, Canada
[c] Electrical Engineering Department, École de Technologie Supérieure, Montreal, Canada
[d] Cyber Security Systems and Applied AI Research Center, Lebanese American University, Lebanon
[e] School of Computer Science and Engineering, Soongsil University, Seoul, South Korea
[f] Avignon University, France
[g] Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

ARTICLE INFO

Keywords:
Contract theory
Internet of vehicles
Secure context prediction
Tidal trust mechanism
Trust rate

ABSTRACT

To ensure better facilitation of vehicular services and improve driving safety in the Internet of Vehicles (IoV), context prediction among vehicles plays a very crucial role. However, as more malicious IoV devices get involved in the network, the context prediction accuracy shared among various servers may degrade severely. Existing schemes have used cryptographic mechanisms to securely and accurately identify malicious devices. However, time and the subsequent delay in identifying and rating the legitimate communicating IoV devices emerge as a crucial issue. Hence, to solve this critical problem, we put forth an efficient and reliable trust framework where trust and context prediction is achieved by Tidal Trust Mechanism (TTM) and Contract Theory (CT). TTM can successfully rate the degree of trust between the devices with a high level of accuracy, whereas CT can verify the context prediction reliably. The proposed mechanism based on TTM and CT ensures that trusted IoV devices are identified with high accuracy and verified reliably. The proposed framework is simulated over real-world data set in MATLAB for various performance metrics, such as altered records, accuracy prediction, response time, and utilities of IoV devices. Simulation results show that the proposed framework provides a significant improvement of approximately 87% in comparison to existing (baseline) approaches while analyzing the accuracy, record alteration, and resource utility among the devices in the network.

1. Introduction

Due to the rapid growth of autonomous vehicles and intelligent devices, the Internet of Vehicles (IoV) is expected to generate a diverse and large volume of information [1]. The Vehicular Ad-hoc Network (VANET) [2] integrated with the Internet of Things (IoT) forms IoV [3], where vehicles are embedded with various smart devices to gather and share information to improve the quality of the intelligent transportation system (ITS) services [4]. With the recent and continuous development in the urban population and expanding cities, autonomous computing machines are rapidly changing our lifestyles, and IoT plays a pivotal role in controlling and analyzing smart devices.

As discussed in the literature, IoT-enabled vehicle automation technologies are prone to various security threats [5]. Security and privacy issues are critical to the success of the IoV. Vehicles will not be willing to share their information over the IoV if the security issues are not sufficiently addressed [6]. Signal processing, machine learning, edge computing, and sensing technologies are used in autonomous navigation, and there exist various safe driving, data collection, and information sharing schemes that improve system robustness and safety in IoV [7,8]. However, the consideration of the proactive behavior of the driver and various safety concerns for context (information) prediction

☆ Peer review under responsibility of Faculty of Engineering, Alexandria University.

* Corresponding author.
E-mail addresses: georges.kaddoum@etsmtl.ca (G. Kaddoum), davidchoi@soongsil.ac.kr (B.J. Choi), abderrahim.benslimane@univ-avignon.fr (A. Benslimane), mmhassan@ksu.edu.sa (M.M. Hassan).

https://doi.org/10.1016/j.aej.2023.07.020
Received 29 April 2023; Received in revised form 28 June 2023; Accepted 10 July 2023
Available online 24 July 2023

remains open. In addition, the various types of context (information) sent among the devices, such as textual, images, audio, and video, may further lead to inviting some intruders to make alterations in the network. Significantly, the involvement of intelligent malicious devices that generate false or modified contexts can slow data gathering and allow unauthorized information access [9–11]. Therefore, a secure context prediction scheme considering the behavioral patterns of vehicles is needed to provide a trusted IoV system.

1.1. Contribution

Many Artificial Intelligence (AI) based schemes have been proposed for accurately predicting behavior or context (information) from IoV [12,13]. However, the existing AI schemes lack interpretability, have high complexity, and are vulnerable to various known security attacks. Moreover, including malicious nodes in IoV adversely affects the network system's accuracy, reliability, and robustness. Therefore, we propose a secure and trusted mechanism for IoV that can effectively detect the involvement of malicious IoV devices by analyzing the context information of the network.

- In particular, we used a trust mechanism based on the tidal trust mechanism (TTM) [14] that can effectively determine the degree of trust of each communicating node and contract theory (CT) [15] that can verify the accuracy and prediction of trusted context prediction. Here, the trust values, varying depending on the communication behavior of IoV nodes, are computed using TTM. The TTM can accurately determine the reliability and security of each IoV device by assigning the trust values based on their communication behavior.
- The nodes with high trust values and rates are included in the communication process. The trust values control the communication process, where the nodes with lower trust and rates do not participate in the communication/opinion of context prediction or analysis process. The trust selector (TS) analyses the generated/collected reports from each IoV device and records the accuracy and reliability of the context prediction. Here, the CT mechanism is used to examine the reports in the network.
- The proposed mechanism outperforms existing works in terms of utilities of IoV, accuracy, identification of altered records, and running/response time as compared to the existing schemes proposed by Kang et al. [16], Guo et al. [8], and Kazmi et al. [15].

The remaining paper is organized as follows. Section 2 describes several existing security approaches proposed by various researchers/scientists. Section 3 presents the proposed framework based on TTM and CT, ensuring a secure and reliable context prediction. Section 4 analyses the result of a proposed framework in comparison with existing schemes. Finally, Section 5 concludes the paper and discusses the future scope of the paper.

2. Related work

2.1. General context prediction mechanisms in IoV

Li et al. [17] proposed a detection algorithm for improving the detection of vehicles using three stages. The algorithm reduces the distortion of the vehicles separating images into various patches. The patches are combined with the original image to create a batch used for detection using a convolutional neural network (CNN). Also, an outlier-aware non-maximum suppression mechanism is proposed to reduce false alarms.

Cebrian et al. [18] proposed a hierarchical scheme for predicting eye fixations. An encode-decoder network is created by merging the visual features through the global–local capsule definition. Also, a learning prediction contextual condition model is developed to estimate visual attention. Their experimental result shows the relationship between local and global contextual conditions and a 29% improvement in information gain compared to existing works.

Kanapram et al. [19] proposed an abnormality prediction/detection scheme based on collective awareness of intelligent agents in the network where the agents are analyzed using a data-driven dynamic Bayesian network. Also, a growing neural gas and Markov jump particle filter approaches are used to learn the conditional probabilities and estimate the state possibilities. The performance analysis is provided in terms of accuracy and reliability.

Liang et al. [20] proposed a scaling-based and feature fusion single shot detector by adding an extra scaling of de-convolution modules to form feature pyramids. Also, detection accuracy and context analysis are improved by incorporating the spatial relationship between objects.

2.2. Secure context prediction methods

Yen et al. [22] provide an analysis of misinformation threats in the network considering the back pressure traffic signal algorithm. Time spoofing and ghost vehicle threats are analyzed to identify the misinformation that can further influence phases of signals. An adversary model was proposed to maximize the disruption among signal phases and formulated a 0–1 knapsack problem to determine the optimal approach. Additionally, hybrid-based and auction-based algorithms are proposed to detect threats or mitigate misinformation issues.

Xia et al. [23] proposed a weighted Markov model and lightweight trust-aware multicast routing schemes. The mechanisms ensure reliable and secure routing paths during handoff processes. Routing metrics are examined against various malicious threats using SUMO, Netlogo, and NS-2 simulators.

Li et al. [24] proposed a blockchain-based vehicular positioning accuracy scheme for ensuring credibility and security among sensors while analyzing the GPS error. Further, they used a deep learning neural network to analyze the error in positioning evolution. The scheme is analyzed for data sharing and error correction metrics to measure the accuracy of the network. Guo et al. [21,25] proposed an intelligent, trusted collaboration mechanism to gather data using unmanned aerial and mobile vehicles. A deadline-aware, trusted collaboration mechanism is proposed to ensure privacy and network security. Also, an AI-based optimization mechanism is proposed to collect the participants' trust. Compared to the existing works, the cost and collection time is reduced by 35.08% and 58.32%, respectively.

Kazmi et al. [15] proposed a contract theory-based incentive mechanism that maximizes the social welfare of vehicular networks by motivating neighboring vehicles to share their resources. They have evaluated the performance of the proposed mechanism compared to the existing scheme against various security threats.

Further, Kang et al. [26] proposed an optimized consensus mechanism using a blockchain network based on contract and reputation-based theory. They designed a secure communication process for vehicular systems.

In comparison with the existing approaches, we propose a secure and trusted context prediction mechanism using TTM and CT where the behavior of the communicating device can be easily traced and identified by computing their trust values. We will show that the proposed mechanism outperforms the three most relevant existing works Guo et al. [21], Kazmi et al. [15], and Kang et al.[26]) against various security metrics. Summary of related work is presented in Table 1. Some existing works are proposed to ensure a secure and trusted communication environment during the transmission of information in the network. However, the existing works may lead to further security concerns due to a decrease in accuracy, an increase in delays, and increased computation and communication overheads. The key management and communication overheads increase the delays and decrease the accuracy of the system. As illustrated in Fig. 1, the proposed mechanism based on an artificial neural network (ANN) provides a secure and trusted communication network where the trust of each

Table 1
Summary of existing context prediction methods.

Authors	Proposed Framework	Method Used	Limitations
Kazmi et al. [15]	contract theory-based incentive mechanism	maximizes the social welfare of the vehicular networks by motivating neighboring vehicles to participate in sharing their resources	Increases storage overhead
Li et al. [17]	Distributed detection algorithm for improving the performance of vehicles detection	Separates images into various patches by cropping to reduce the distortion of the vehicle	Provides untrusted scenarios
Cebrian et al. [18]	Hierarchical scheme for predicting eye fixations	Uses learning prediction contextual condition model to estimate visual attentions	Increases communication overhead during transmission
Kanapram et al. [19]	Collective awareness of intelligent agents	Uses data-driven dynamic Bayesian network to predict/ detect abnormalities	Increases the key management, and communication overheads
Liang et al. [20]	Feature fusion and scaling-based single shot detector	Uses spatial context analysis to improve detection accuracy	Requires delay in analysis
Guo et al. [21]	Intelligent, trusted collaborative mechanism	A deadline-aware trusted collaboration mechanism to ensure privacy in the network	Increases the communication overhead
Kazmi et al. [15]	Contract theory-based incentive mechanism	Maximizes the social welfare of the vehicular networks	Increases computational overhead
Yen et al. [22]	Backpressure traffic signal algorithm	Analyzes time spoofing threat and ghost vehicle threat using TSC algorithm to identify the misinformation that influences the phases of signals	Incurs long delays in legitimate device identification
Xia et al. [23]	Trusted routing scheme	Analyzes secure routing path using lightweight and Markov model schemes	Incurs long delays while identifying the malicious threats
Li et al. [24]	Blockchain based Scheme	Analyzes the accuracy while sharing the information	Has large communication and storage overhead

device is computed regularly to reduce the delays in contextual transmission. The communications from devices having sufficiently high trusted values are trusted in the network. In addition, fast trust computation leads to higher accuracy and reliability in the network, which further improves the communication process.

3. Proposed framework

The TTM is used to determine the reliability and security of each IoV device by assigning the trust values based on their communication behavior. The trust values are used to control the communication process. The nodes with high trust values and rates are included in the communication process. The nodes with lower trust and rates do not participate in the communication/opinion of context prediction or analysis. As many abbreviations and symbols are used in the paper, they are listed and described in Table 2.

3.1. Real time secure prediction of IoV

There are a total of n IoT-enabled vehicular devices in the system, where a subset is assumed to be malicious. The proposed framework determines the nodes' accuracy and behavior in three stages, as illustrated in Fig. 1. Initially, while establishing the network, all the nodes are assumed to be legitimate. Compromised trusted nodes become malicious nodes that may degrade the network performance. Here, the degree of trust of each communicating node is determined using TTM consisting of two repeated phases. In the first phase, the level-wise rating and trust of all nodes are computed for the *current level* (level i), where the *next level* (level $i+1$) is further computed using level i. Here, the level refers to the separation of devices depending upon their arrangement or establishment in the network, as shown in Fig. 2. In the second phase, each node computes the trust value of neighboring nodes and chooses the node with the highest trust value to transmit. The first stage involves communication among vehicles, representing the transmission process having storage, exchanging, and information sharing. The second stage, TTM [27] for trust computation, is used to compute and analyze the trust of each communicating device using the tidal trust model. Finally, stage 3 provides accurate decisions and predictions using context theory prediction.

3.1.1. Secure communication using TTM

The vehicular network is represented using a graph where the vertices are the IoV nodes connected using bidirectional edges. Initially, a uniformly distributed trust value $(TV) \in [0,1]$ is randomly chosen for each node. *TV* increases or decreases depending on their future communication behavior. *TV* of each node is recorded in a trust selector database by the IoV devices. Each node calculates the *TV* of neighboring nodes in each level. The *TV* calculation is updated after receiving the context information from other IoT devices. The *TV*s of nodes in the current level are calculated using the *TV*s from the previous level. If a node has more than one predecessor, the maximum of the *TV*s of its predecessors is chosen to be the *TV*.

An example case is shown in Fig. 2.

a) **Level 0**: The *TV* of node Q is 0.65 because the *TV* of node P, its only predecessor, is 0.65. Similarly, the *TV*s of nodes R and S are inherited from node P and are 0.60 and 0.70, respectively. After the *TV*s of all nodes in level 0 are computed, the TTM continues to level 1 to compute the *TV*s of all nodes in level 1. The trust values assigned to each node depend on the behavior or information transmission rate in the network. However, the ratings of each node determine the opinion of a node about its legitimacy and malicious behavior towards its neighboring nodes.
b) **Level 1**: The *TV*s from level 0 will be used to compute *TV*s in level 1. The *TV* of node T is calculated using the *TV*s of its predecessors Q and R. R has rates T with the minimum ratings, such as (0.60), and its trust towards T (0.70), i.e., 0.60. Q rated T with the minimum rating (0.65), and its trust towards T (0.65) is 0.65. The final rating of T is the minimum between these two ratings, and its value is 0.65. Similarly, the ratings of Q, R, and S are (0.65), (0.60), and (0.70), respectively. Their trust towards U is (0.60), (0.70), and (0.65), respectively. Now, the final rating of U is the minimum among these three ratings, i.e. (0.60).
c) **Level 2**: The *TV* towards node V will be 0.50, the minimum rating by node T (0.60) and node U (0.50). The remaining process continues recursively as Breadth-First Search (BFS) by dynamically establishing the threshold among source and destination. If a node acts malicious, its rating and *TV* would always be less and discarded during communication.

Further, the contract theory is used to model context prediction during interactions between trusted and malicious IoV devices where accuracy and prediction are considered. The neighbor with the

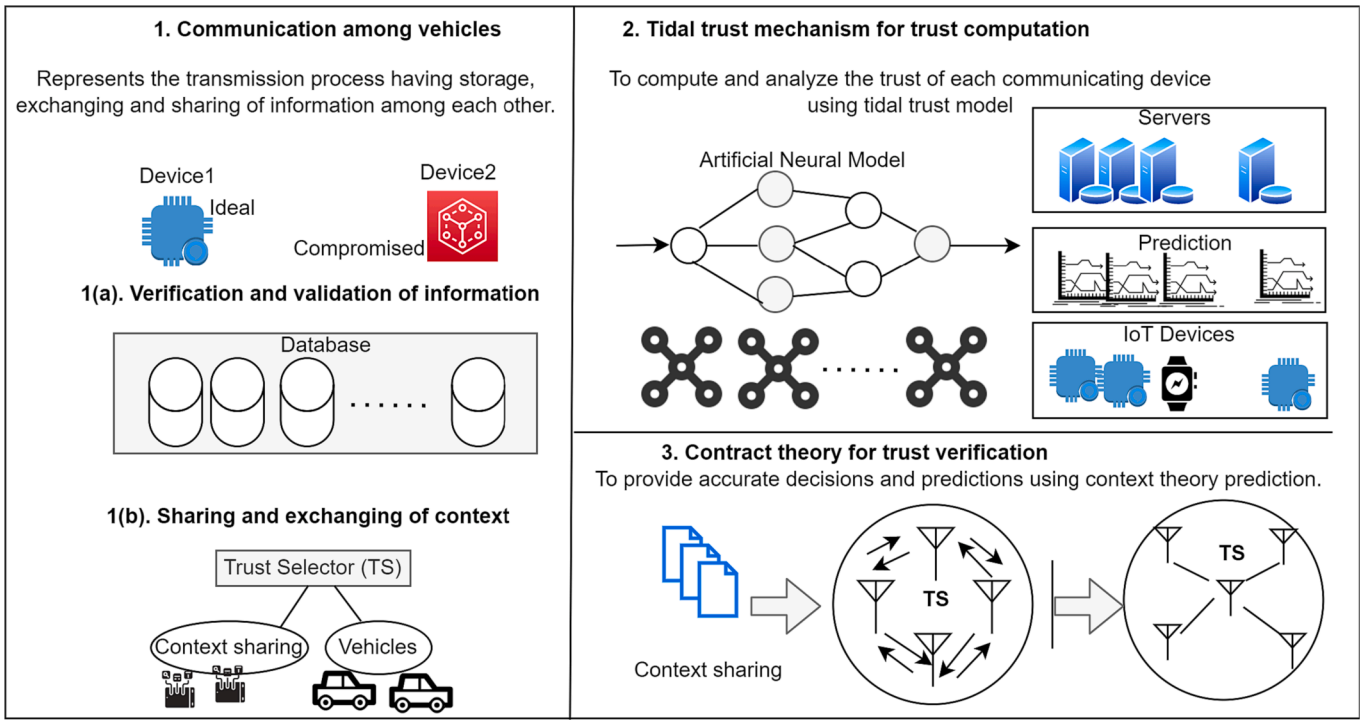

Fig. 1. Overall process of the proposed framework to achieve high accuracy and reliability.

Table 2
List of symbols and abbreviations.

Symbol	Description
CA_n^m	Context accuracy of node n computed by verifier m
CMR	Commutative Measure Rate
$Context_n^m$	Context of resource for the verification of node n by verifier m
CT	Contract Theory
IF	Interaction Effects
IoV	Internet of Vehicles
IT	Interaction Timeless
n	Index of IoT device/node $\in \{1,\ldots,N\}$
PA	Predicted Accuracy
PH	Previous History
ϕ_k	Latency matrix of type-k nodes
PMR	Present Measured Rate
R_k^{max}, L_k^{-1}	Optimized profit and latency via verification
TR_n^d, TR_n^u	Downlink and uplink Shannon capacity
TS	Trust Selector
TTM	Tidal Trust Mechanism
T_k	Verification time of result broadcasting
T_n	Transmission time of unverified device
TV	Trust Value
$U_{bn}(k)$	Profit of TS using type-$-k$ nodes
U_k	Utility Function

minimum TV is chosen to transmit.

3.1.2. Context prediction using contract theory

After identifying the trusted nodes using TTM, verifying the accuracy and prediction of context is still needed. An incentive is given to the IoV devices to motivate them to take part in the context verification process. Participants are rewarded for accomplishing its task accurately and honestly. However, the availability of prior knowledge of devices that participate in the verification process is not always guaranteed. Also, there can be compromised nodes that share inaccurate information with others. Therefore, incentivizing the well-behaved nodes during the verification process can help to mitigate these problems. To design a reliable and accurate incentive mechanism, we adopt a CT-based mechanism that can verify the legitimacy of each communicating node in the network.

To verify node $n \in \{1,\ldots,N\}$, consider a Trust Selector (TS) that acts as context publisher and a set of trust verifiers defined as $V = \{V_1, V_2, \ldots, V_N\}$ that include both legitimate and compromised nodes. The trust verifiers are willing to contribute various computational resources, such as processing time to execute node trust verification, defined as $R = \{r_n^1, r_n^2, \ldots, r_n^m\}$, where m represents a trust verifier. The transmitted and verified values of TV of node n are denoted as T_n and O_n, respectively. For a trust verifier m, the context of resource for the verification of node n denoted as $context_n^m$ having n number of IoT devices. A three-tuple is

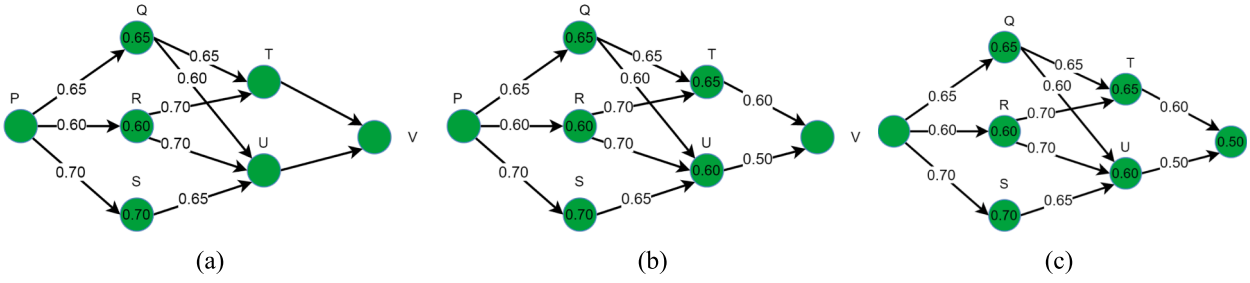

Fig. 2. TTM Levels (a) Level 0, (b) Level 1, and (c) Level 2.

used for verifying the context accuracy, defined as

$$CA_n^m = (context_n^m, n, O_n). \tag{1}$$

The trust values are sorted in ascending order as $K_1 < K_2 < \ldots < K_k$, where k represents various trust values of nodes in the network. The larger K_k implies a higher trust value. Different IoV devices have different trust values; the TS offers the trust a contract as $(R_k(L_k^{-1}), L_k^{-1})$ that defines a series of latency incentive bundle, where L_k is the latency of verification of trust of type-k node and L_k^{-1} is the reciprocal of L_k. The corresponding incentive is $L_k R_k(L_k^{-1})$.

3.1.3. Latency in trust verification

To verify each IoV device's trust value, each device executes the following four verification processes:

- A list of unverified trust node transmission from TS to devices.
- Verification of local trust.
- Broadcasting of verification results and comparing between devices.
- Transmission of verification feedback from devices to TS.

For a trust verifier V, the latency consisting of corresponding delays of the steps above is calculated as:

$$L_k(context_n^m, T_n, O_n) = \frac{T_n}{TR_n^d} + \frac{context_n^m}{r_n^m} + \psi T_k|V| + \frac{O_n}{TR_n^u}, \tag{2}$$

where TR_n^d and TR_n^u are the downlink (from TS to IoV devices) and uplink (from IoV devices to TS) transmission rates, respectively, T_n/TR_n^d is the transmission time of unverified device from TS to IoV device, $context_n^m/r_n^m$ is the local verification time. Here, T_k and V determine the verification time of the result from value broadcasting and comparison with a network size k and V IoV trust verifier, where ψ is the predetermined verification result calculated using the statistics of the previous verification process. O_n/TR_n^u is the verification feedback time. The TR_n^d and TR_n^u are computed using the Shannon capacity for TDM operating on the same frequency channel as [26]:

$$TR_n^d = TR_n^u = TB\log_2\left(\frac{1 + \overline{P_n}|C_n|^2}{\sum_{n \notin V}^{n} \overline{P_n} - |C_n^-|^2 + D_0 TB}\right), \tag{3}$$

where TB is the transmission bandwidth and $\overline{P_n}$ is the transmission power to node n. C_n is the channel gain of peer-to-peer links among node n and TS. D_0 is 1-sided spectral density level of Gaussian node and n- is the element of V excluding n. Further, according to the signed contract $(R_k, L_{k^{-1}})$ among TS and type-k^- node, the profit of TS obtained from type-k^- node is computed as:

$$U_{bn}(k) = \pi[\phi_k(L_k)] - lR_k, \tag{4}$$

where l is predefined trust values determined using TTM for type-k nodes having an incentive value of $R_k, \pi[\phi_k(L_k)]$ is the TS benefit regarding latency matrix ϕ_k for type-k^- nodes. The latency metric is used to balance the network scaling, and verification time is expressed as the below equation:

$$\phi_k = \begin{cases} e_1(K_k|V|\rho_k)^{z1} - e_2(\frac{L_k}{T_{max}}), & \text{if} 0 < L_k < A, \\ 0, & \text{otherwise}, \end{cases} \tag{5}$$

where $A = \frac{T_{max} e_2^{z2-1} (K_k|V|\rho_k)^{\frac{z1}{z2}}}{e_2^{z2-1}}, e_1 > 0$, and $e_2 > 0$ are predefined coefficients network latency for ensuring the block verification, ρ_k is the prior probability of type-k device where $\sum_{k=1} KP_k = 1$, and T_{max} is the maximum tolerable verification latency indicating the effects of verification latency and scale of trust verification. The objective of the TS is to maximize, through verification, the profit defined as:

$$(R_k^{max}, L_k^{-1}) U_{bk}(k) = \sum_{k=1} K(|V|\rho_k)(\pi[\phi_k(L_k)] = lR_k), \tag{6}$$

where R_k is defined as the incentive value of the type-$k$device. On the other hand, the objective of the type-k device is to maximize the utility function of each trust verifier k defined as:

$$(R_k^{max}, L_k^{-1}) = U_k = K_k\eta(R_k) - l' L_k^{-1}, \forall k \in \{1, \ldots, K\}, \tag{7}$$

where $\eta(R_k)$ is a monotonically increasing valuation function of type-k^- depending on the value of incentive R_k, and l' is the cost of trust verification of each resource, including network resource and computation resource overhead.

3.1.4. Designing of optimal contract

To generate a feasible contract, each contract item for devices must satisfy the following three basic properties:

1. *Individual Rationality (IR)*: Each device joining the verification process receives a positive utility as:

$$K_k\eta(R_k) - l\ L_k \geqslant 0, \forall k \in \{1, \ldots, K\}.$$

2. *Individual Context (IC)*: type-k^- device can only receive maximum utility when selecting the contract designed for themselves as $(R_k^{'}, L_k^{-1})$:

$$K_k\eta(R_k) - l\ L_k \geqslant K_k\eta(R_k) - l' L_k^{-1}, \quad \forall K\ \notin\ k, k^{'} \in \{1, \ldots, K\},$$

where $R_k^{'}$ represents the maximum utility.

3. Here, we have considered $\pi[\phi_k(L_k)] = g_1\left[e_1(K_k/V/P_k)^{z_1} - e_2(\frac{L_k}{T_{max}})^{z_2}\right]$ for the ease of presentation. z_1 and z_2 are the given factors for scaling and latency while verifying the block.

Finally, the optimization problem as $\text{argmax}_{k \in K} L_k$ is formulated as follows:

$$\begin{aligned} &\mathbf{P1}: \text{maximize}\left(R_k, L_k^{-1}\right) U_{bk} \\ &= \sum_{k=1} K|V|\rho_k\left[g_1 e_1(K_k|V|\rho_k)^{z_1} - g_1 e_2 \frac{L_k}{T_{max}}^{z_2}\right] - lR_k, \end{aligned} \tag{8a}$$

s.t.

$$K_k\eta(R_k) - l' L_k^{-1} \geqslant 0, \forall k \in \{1, \ldots, K\}, \tag{8b}$$

$$\begin{aligned} &K_k\eta(R_k) - l' L_k^{-1} \geqslant K_k\eta(R_{k'}) - l' L_{k'}^{-1}, \\ &\forall k \in \{1, \ldots, K\}, k' \notin \{1, \ldots, K\}, \end{aligned} \tag{8c}$$

$$Max L_k \leqslant T_{max}, \forall k \in \{1, \ldots, K\}, \tag{8d}$$

$$\sum_{k=1}^{K} \rho_k R_k \leqslant R_{max}, \forall k \in \{1, \ldots, K\}. \tag{8e}$$

The condition specified in Eq. (8b) guarantees a positive utility function among all legitimate nodes in the network, Eq. (8c) maximizes the utilization of type-k^- devices in the network and categorizes the devices, including the particular context in the network, Eq. (8d) categorizes all the devices having maximum latency while verifying the trust in the network, and Eq. (8e) categorizes the incentive values of all type-k devices in the network, where R_{max} is the given transaction fee from ITS device.

Algorithms 1–4 show the technical details of the proposed

framework. They show the details of different modules functioning together to provide a secure and efficient system (Algorithm 1: Identification and Verification of Trust Computation, Algorithm 2: Tidal Trust Mechanism (TTM), Algorithm 3: Level Trust, Algorithm 4: Contract Theory).

Algorithm 1. Identification and verification of trust computation

Require: All stages/phases of nodes are represented in the graph network.
Input: (1) Number of IoV devices d, (2) 2 states (trusted or malicious)
Output: Device is either trusted or in the malicious state
Step 1: Initially, assign a random trust value to all IoV devices $\in [0,1]$
Step 2: Execute *Tidal Trust Mechanism (TTM)* (Algorithm 2)
Step 2: Execute *Level Trust* (Algorithm 3)
Step 3: Execute *Contract Theory (CT)* (Algorithm 4)

Algorithm 2. Tidal Trust Mechanism (TTM)

Require: All stages/phases of nodes are represented in the graph network.
Input: (1) Number of IoV devices d, (2) 2 states (trusted or malicious)
Output: Device is either trusted or in the malicious state
Step 1: Compute the TV of each IoV device based on the history of interactions
Step 2: Update the trust of level $i+1$ from level i

Algorithm 3. Level Trust

Require: All stages/phases of nodes are represented in the graph network.
Input: (1) Number of IoV devices d, (2) 2 states (trusted or malicious)
Output: Device is either trusted or in the malicious state
Step 1: Initially, assign rating and TV to node i at level i
Step 2: If device_i has more than one input from level i, **then** trustdevice_i (at level $i+1$) is computed as:
trustdevice_i (at level $i+1$) $\leftarrow$ $min(\text{device}_i(TV), \text{device}_i(rating)\text{trustdevice}_i \leftarrow max(TV(\text{device}_1, \text{device}_2, \ldots, \text{device}_i))$
Step 3: Compute the trust among each IoV device_i as:

$$t_{ni}, \text{device}_i = \frac{t_{n_{ij}} \times t_{j\text{device}_j} | t_{ij} > max}{t_{n_{ij}} | t_{ij} \geqslant max}.$$

Algorithm 4. Contract Theory (CT)

Require: All stages/phases of nodes are represented in graph network
Input: (1) Number of IoV devices d, (2) 2 states (trusted or malicious)
Output: Device is either trusted or in the malicious state
Step 1: Compute the contract accuracy as in Eq. (1)
Step 2: Compute latency of trust verification as in Eq. (2)
Step 3: Compute the profit of TS as in Eq. (4)
Step 4: Compute the latency of security matrix as in Eq. (5)
Step 5: Compute the maximized profit as in Eq. (6)

All the algorithms mentioned above present the individual working of each security scheme, such as trust computation, TTM, and level trust that determines the complete description of the algorithms above. The formula mentioned in Algorithm 3, "Level Trust," is used to analyze the category of communicating device by comparing it with a maximum threshold that other entities will decide.

4. Performance analysis

Table 3 and Table 4 show the simulation parameters and the predefined values used for evaluation. The data set of real-world San Francisco Yellow Cabs [16] is used in our simulation. In the data set, the mobility of 536 taxis was recorded for a month. In our MATLAB simulation environment, 200 IoV devices in a 500 m × 500 m area change their decisions every 60 s. The mobility rate of each IoV device varies between 40–100 km/h based on weather and congestion conditions. Initially, each IoV device is assigned a random trust value that changes depending on TTM. Moreover, the context prediction accuracy of IoV devices is verified using a contract theory.

Table 3
Simulation parameters of framework.

Parameter	Value
Observation area	500 m × 500 m
Number of IoV devices	200
IoV speed	[40, 100] km/h
Weight values	$\alpha = 0.6, \rho = 0.4$
Rate of compromised IoV	[5, 50]%
Trust values	[0, 1]
Transmission power	[10, 23] dBm
Receiver power	14 dBm
Computational resources	10^3 CPU cycle/unit time

Table 4
Predefined values.

Parameter	Value
Pre-defined metrics1	$g_1 = 1.02, e_1 = 10, e_2 = 8$
Pre-defined metrics2	$z_1 = 1.5, z_2 = 1$
Pre-defined metrics3	$l = 4.5, l' = 1, T_{max} = 250$ s
Pre-defined metrics4	$R_{max} = 1000, \phi = 0.5$

As depicted in Table 4, the values $g_1, e_1, e_2, z_1, z_2, l, l', T_{max}$, and R_{max}, respectively, represents profit gain, network scaling, latency, factors affecting scaling, latency, weight gain, resource cost, transmission cost, maximum tolerance latency, and transaction fee.

4.1. Evaluation metrics

The detailed evaluation metrics such as interaction rate, interaction effect, and previous history are the factors that are considered while computing the trust of and prediction of each node. Along with TTM, the trust value depends on the number of devices communicated and affected while transmitting the information. So, the weight values in the simulation are used to compute and analyze the trust value during the establishment and communication process of the network. The unusually more active devices are generally considered malicious devices whose records are simultaneously recorded and stored as the previous history. The system can directly check the database records and the effect of interactions during the prediction and accuracy to reduce the communication among them. The evaluation metrics explain the factors that can be considered while directly predicting the nature or type of a device during the communication process. The following metrics are used by TTM to calculate the trust values of IoV, which change depending on the context prediction.

Interaction Rate (I_{rate}): The interaction rate among m malicious nodes over a total number of nodes n is defined as the amount of time the opinion of a node changes for its neighboring nodes as the ratio between the legitimate node and all the nodes computed as:

$$I_{rate} = \sum_{j=1}^{m} \frac{\text{legitimate}}{\text{legitimate} + \text{malicious}}. \tag{9}$$

The trust value of a node, either legitimate or compromised, to its neighboring devices impacts the opinions of succeeding nodes. The term opinion is specifically relevant to the communication process where the nodes with lower trust and rates do not participate in the communication/opinion of context prediction or analysis process.

Interaction Effect (I_{effect}): The number of positive and negative opinions by legitimate or malicious devices during the communication process, computed as:

$$I_{effect} = \frac{\text{positive opinion}}{\text{positive opinion} + \text{negative opinion}}. \tag{10}$$

The term opinion is specifically relevant to the communication process where the nodes with lower trust and rates do not participate in the

communication/opinion of context prediction or analysis process.

Previous History (PH): The trust opinion of a neighboring node can be decided by checking its previous history record or trusts provided by its neighboring nodes, computed as:

$$PH = \sum_{i=1}^{n} (EC + F_p + R_p + CT), \tag{11}$$

where EC, F_p, R_p, and CoT are defined as the energy consumed, forwarding packets, receiving packets, and constant time required by each node during information transmission, respectively.

The communicative measure rate (CMR) is used to analyze the communication time while identifying the trust of each node using various predefined metrics. The CMR is mentioned as the metrics m_i at time t that can be measured as the ratio of CMR at $t-1$ over the number of rates measured by metrics m_i as:

$$CMR^{t}_{m_i} = \frac{CMR^{t-1}_{m_i} + PMR^{t}_{m_i}}{n^{t-1/2}_{m_i} + 1}, \tag{12}$$

where $PMR^{t}_{m_i}$ is the present measured rate of metric m_i at time t and $n^{t-1}_{m_i}$ is the measured rates for metrics m_i up to time $t-1$.

4.2. Baseline Schemes

We have compared the performance of the proposed framework with the two baseline approaches. The performance of the proposed mechanism is compared with the works by Xing et al. (Baseline Scheme 1: IEEE TVT, 2022) [28] and Kumar et al. (Baseline Scheme 2: IEEE TVT, 2022) [29], where the trust opinion of each IoV device is computed using various security mechanisms. They use cryptographic primitives to ensure the security of IoV context prediction with additional security cost, time, and delay. In addition, we have added a recent paper in our comparison, Kazmi et al. (Baseline Scheme 3: IEEE TITS, 2021) [15]. They use a contract theory mechanism to determine the accuracy and security of Cooperative Task-Offloading in Electrical Vehicular Networks. On the contrary, the proposed mechanism provides the accuracy and security of IoV context prediction using computation mechanisms. The TTM and the CT together ensure trust and accurate information transmission among nodes in the network while verifying the context and legitimacy of each node by computing the context accuracy of each information and device in the network. Fig. 3 depicts the overview of the proposed framework using TTM and CT. The context of each device n is predicted using TTM and verified by a number of verifiers m using CT. As a result of the proposed framework, based on the different degrees of trust represented by k, each IoV device is identified as trusted or malicious. The different layers represent the way communication process occurs among devices depending upon their behavior. The number of IoV devices depending upon their metrics (behavior) rated according to Tidal Trust Mechanism that is again marked as legitimate and malicious according to internal communication computations using contract theory and trust selector. The devices are typed into various types as type 1, type 2,…type n.

4.3. Results and discussions

The TS acts as a context accuracy publisher measured by various IoV devices. Each IoV selects a contract item (R_k, L_k^{-1}) to sign and verify the recorded trust opinion.

The resource cost unit of $I' = 1$ corresponds to a relatively low vehicle speed of 40 km/h. the resource cost and the vehicular speeds are directly proportional to each other. The more vehicular speed corresponds to the high and continuous consumption of resources required to ensure a secure and efficient communication system. Fig. 4 shows the comparison of utilities between different IoV types: type-0 (legitimate), type-1 (malicious), type-2 (highly malicious), and type-3 (sensitive). Each IoV records its trust value using contract theory and submits it to TS to identify the accuracy of its context-sharing prediction. In addition, We can observe a larger utility at higher speeds and a smaller utility at slower speeds. This is because various trust rates are provided by the proposed mechanism schemes, such as TTM, CT, and TS, to each IoV device. The higher vehicular speed results in negative communication quality, interaction delay, frame loss, etc. The legitimate nodes have the lowest utility rate, and sensitive devices have the highest utility rate because the utility function is increased by intruders altering or modifying the transmitted information. The utility function of sensitive devices is higher as they are more active in the network and can be easily traced in the environment.

Fig. 5 compares utilities for different vehicular speeds. We can observe a larger utility at higher speeds and a smaller utility at slower

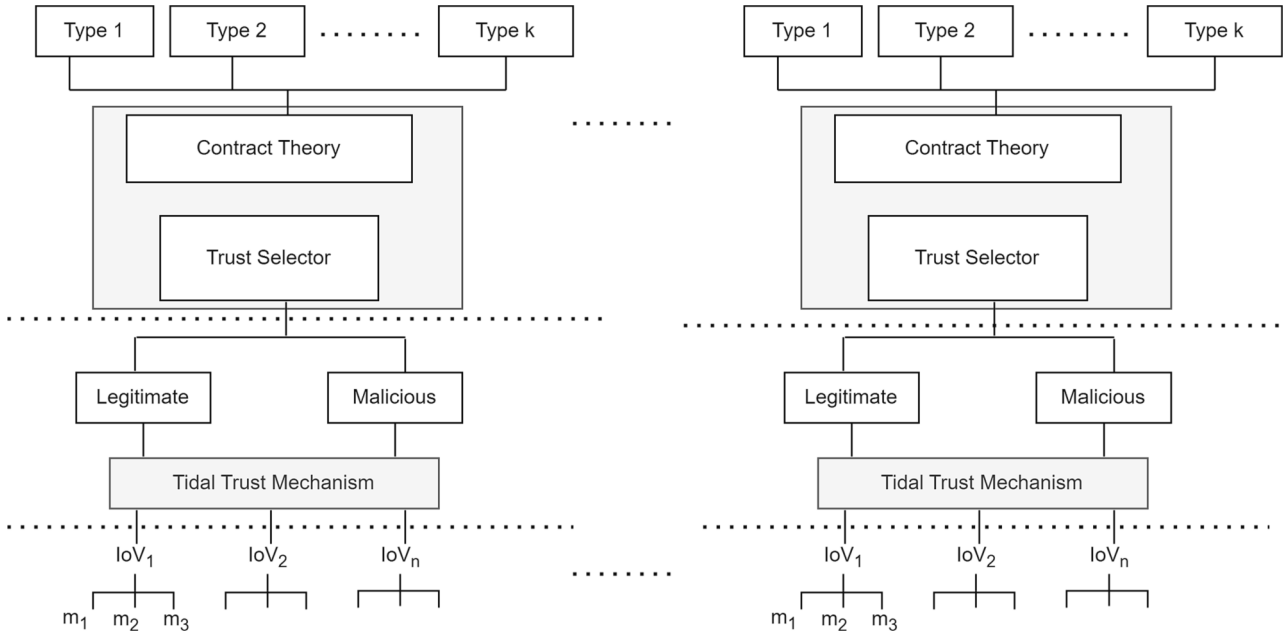

Fig. 3. Overview of the proposed framework using TTM and CT.

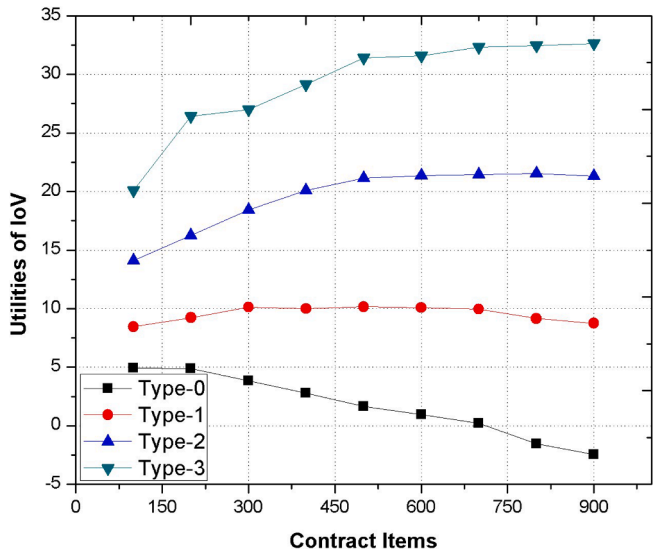

Fig. 4. Utilities of IoV.

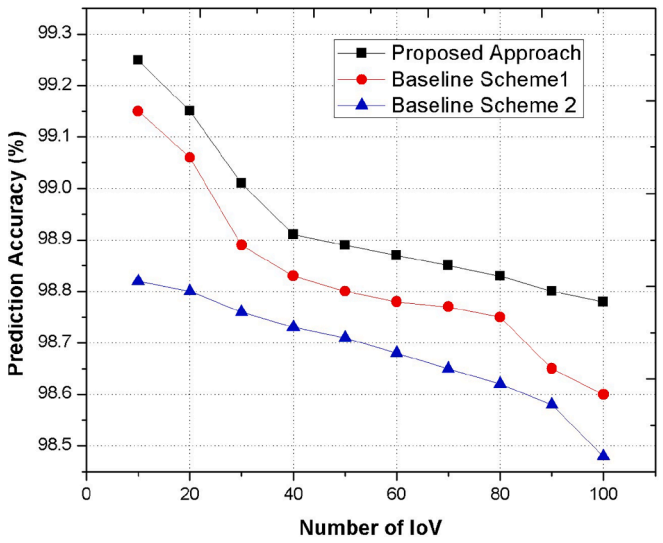

Fig. 6. Comparison of predicted accuracy.

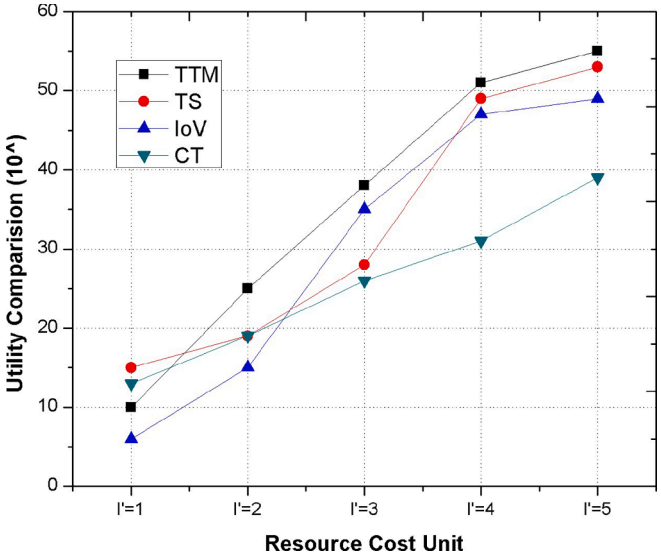

Fig. 5. Utility comparison among various schemes.

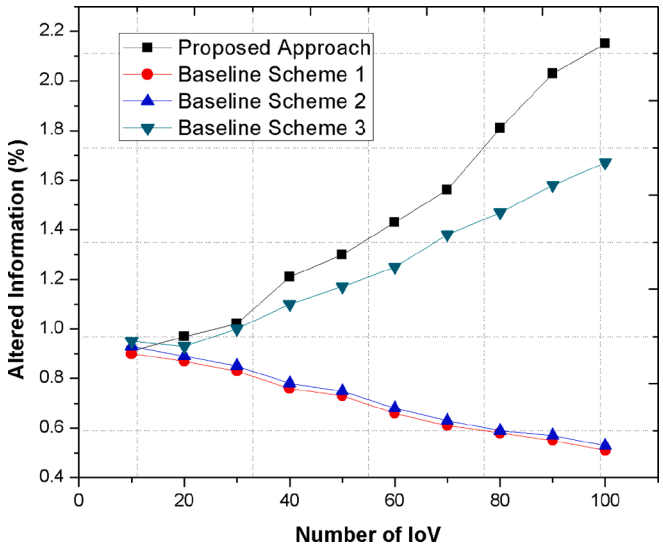

Fig. 7. Comparison of altered records.

speeds. This is because various trust rates are provided by the proposed mechanism schemes, such as TTM, CT, and TS, to each IoV device. The higher vehicular speed results in negative communication quality, interaction delay, frame loss, etc.

Fig. 6 shows the prediction of context accuracy by TS recorded from various IoV devices. The context accuracy of highly trusted devices is accurate and correct compared to less trusted values. The reason is that TTM distributes and changes the trust value and rating of each IoV device before applying the contract theory to measure the reliability of the network efficiently.

Fig. 7 shows the effect of transmitted information by altering the IoV devices from legitimate to malicious. During the network establishment where intruders may compromise or alter the devices to degrade the accuracy of the system. In addition, high-speed IoV devices can be easily traced and altered by intruders as it is critical to record their accurate information by the system. The proposed mechanism significantly outperforms the existing mechanisms by using the trust values and rating evaluations and selecting accurate information among the network nodes.

Finally, Fig. 8 shows the running time of the proposed framework for various IoV devices. We can observe that the running time increases linearly with the number of devices. Therefore, the proposed framework is scalable and can be applied to large networks.

4.4. Confidence model

The proposed mechanism is further analyzed and validated against false positive and false negative rates against two more recent existing approaches. Xing et al. [28] considered as Baseline Scheme 1 have proposed a secure delivery service for the content based on the formation of the game. Authors have proposed a secure, private content delivery mechanism protecting sensitive information. In addition, the authors have proposed an incentive-based connected and autonomous vehicular approach by conducting extensive demonstrations and simulations against various metrics. Kumar et al. [29] considered as Baseline Scheme 2 have designed a deep learning and blockchain-based security model by registering and verifying all the communicating entities. The proposed mechanism uses a contract-based byzantine fault tolerance scheme to authenticate the data. In addition, the deep learning scheme is used to analyze the behavior of intruders using various simulation models.

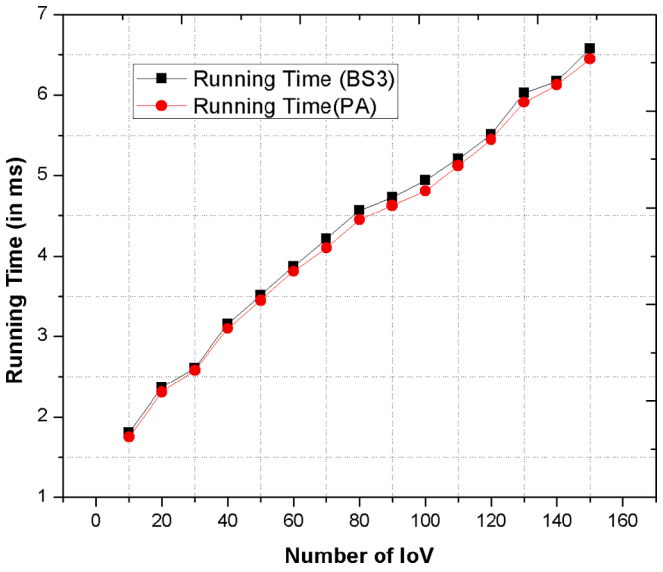

Fig. 8. Running time of proposed approach.

The confidence model determines the reliability and vulnerability of the communicating network while transmitting the information from source to destination. In this paper, the false positive and false negative rates are used to validate and verify the proposed mechanism against recent existing security approaches. False positive rates represent the percentage of devices the intruders alter while the system identifies them as legitimate. However, a false negative rate occurs when the system identifies them as legitimate devices, where these devices are malicious and altered by intruders. Both approaches are analyzed over false positive and false negative rates.

Fig. 9 depicts the false positive result that shows the outperformance of the proposed system against Xing et al. [28] and Kumar et al. [29] as the proposed mechanism used tidal trust approach to surveillance and analyze the communicating behavior of each device in the network.

In addition, Fig. 10 represents the false negative scenario where the legitimacy of each communicating device is further recognized using a context theory scheme that identifies the malicious behavior of any device before starting the information transmission process in the network. The proposed mechanism provides significant results as compared to both the existing schemes.

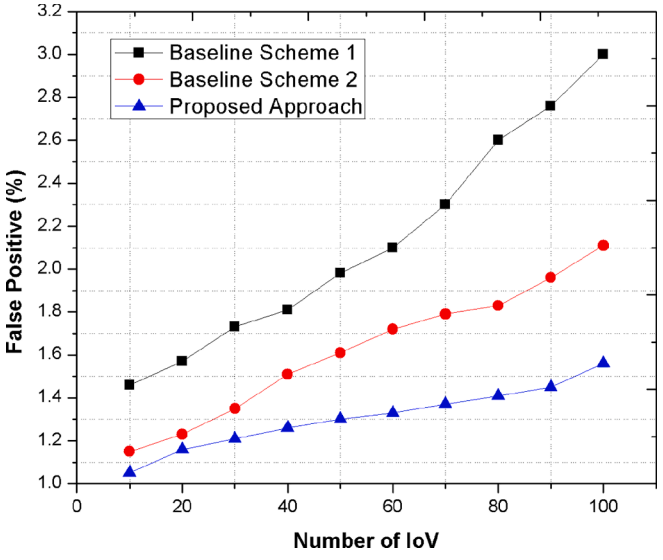

Fig. 9. False positive rate.

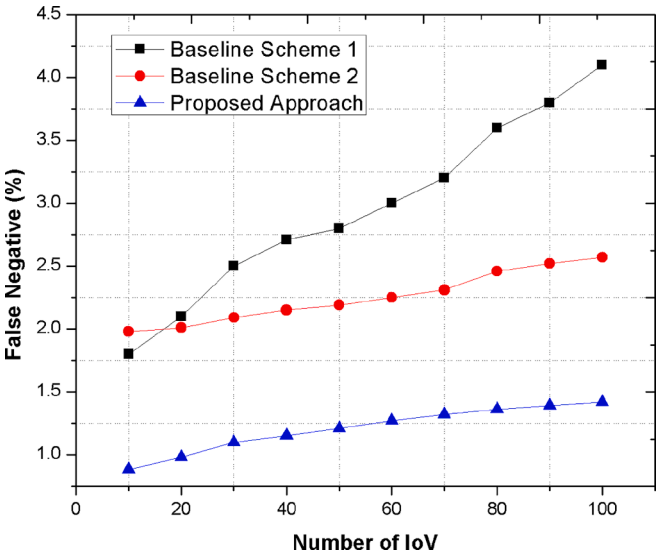

Fig. 10. False negative rate.

The proposed mechanism successfully outperforms the baseline approaches, providing better accuracy, higher confidence, and preventing records from alteration. The tidal trust mechanism and contract theory are the two prediction approaches while identifying the legitimacy of communicated device. The complexity of the proposed phenomenon is $O(n)$ as $n+n^2$ number of legitimate devices are allowed to communicate among each other. All the devices can't be trusted at the same time as we are validating the proposed phenomenon.

4.5. Complexity analysis

To identify the user (either legitimate or malicious) when the device analyzes a node's activity, the TTM will communicate with $(n-1)$ devices, i.e., it will conduct $(n-1)$ trials to verify the legitimacy of a node. The time complexity of the proposed algorithm is, therefore, $O(\log(n-1))$. However, the context analysis and trust evaluation are repeated at least n times in the existing approach. There is also associated communication cost. Therefore, the minimum complexity of the existing approaches give $O(n \times (\log(n-1)))$.

4.6. Summary

The proposed framework illustrates a secure communication environment for autonomous vehicles where devices can intelligently communicate with a higher trust rate. The tidal trust mechanism and context theory are used to compute the accuracy and verify the record alteration by the intruders while transmitting the information in the network. The device having a higher trust value can transmit the information and ensure reliability in the context of the records. In all the predicted results, the proposed mechanism outperforms baseline schemes. This is because a highly trusted environment is maintained with low computational delays. After all, only the devices with higher trust values are involved in the communication process. Further, the systems increase accuracy and reliability because contract theory continuously verifies the measured parameters.

5. Conclusion

The proposed mechanism introduced an efficient and reliable context prediction framework using the tidal trust mechanism and contract theory. The proposed framework assigns the trust values to each IoV device, which is further used to analyze the accuracy of context prediction among several devices. The proposed framework validated

the effectiveness and accuracy of existing schemes against various measuring metrics. The proposed mechanism outperforms identifying the altered record shared by compromised devices in the network. In addition, the proposed mechanism achieves better utility, accuracy, and response time. The number of the dynamic behavior of the IoV network can be further analyzed by computing more weights considering several intrinsic mechanisms in future considerations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was supported by the MSIT Korea under the NRF Korea (NRF-2022R1A2C4001270) and the Innovative Human Resource Development for Local Intellectualization support program (IITP-2023-RS-2022–00156360) supervised by the IITP. This work was also supported by the King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP2023R18.

References

[1] M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.
[2] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, VANET security challenges and solutions: a survey, Vehic. Commun. 7 (2017) 7–20.
[3] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," Inventions, vol. 4, no. 1, 2019, article 22.
[4] G. Rathee, F. Ahmad, F. Kurugollu, M.A. Azad, R. Iqbal, M. Imran, CRT-BIoV: A cognitive radio technique for blockchain-enabled internet of vehicles, IEEE Trans. Intell. Transp. Syst. 22 (7) (2020) 4005–4015.
[5] A.U. Makarfi, K.M. Rabie, O. Kaiwartya, K. Adhikari, G. Nauryzbayev, X. Li, R. Kharel, Towards physical layer security for internet of vehicles: Interference aware modelling, IEEE Internet Things J. 8 (1) (2020) 443–457.
[6] R. Elhabob, Y. Zhao, I. Sella, H. Xiong, Efficient certificateless public key cryptography with equality test for internet of vehicles, IEEE Access 7 (2019) 68 957–68 969.
[7] W. Wang, F. Xia, H. Nie, Z. Chen, Z. Gong, X. Kong, W. Wei, Vehicle trajectory clustering based on dynamic representation learning of internet of vehicles, IEEE Trans. Intell. Transp. Syst. 22 (6) (2020) 3567–3576.
[8] J. Guo, S. Kim, H. Wymeersch, W. Saad, W. Chen, Guest editorial: introduction to the special section on machine learning-based internet of vehicles: theory, methodology, and applications, IEEE Trans. Veh. Technol. 68 (5) (2019) 4105–4109.
[9] T.A. Butt, R. Iqbal, S.C. Shah, T. Umar, Social internet of vehicles: Architecture and enabling technologies, Comput. Electr. Eng. 69 (2018) 68–84.
[10] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," Sensors, vol. 19, no. 14, 2019, article 3165.
[11] D. Gupta, S. Rani, B. Tiwari, T.R. Gadekallu, An edge communication based probabilistic caching for transient content distribution in vehicular networks, Scientific Reports 13 (1) (2023) 3614.
[12] G. Rathee, R. Sandhu, H. Saini, M. Sivaram, V. Dhasarathan, A trust computed framework for iot devices and fog computing environment, Wireless Netw. 26 (4) (2020) 2339–2351.
[13] Z. Ning, Y. Feng, M. Collotta, X. Kong, X. Wang, L. Guo, X. Hu, B. Hu, Deep learning in edge of vehicles: Exploring trirelationship for data transmission, IEEE Trans. Industr. Inf. 15 (10) (2019) 5737–5746.
[14] J.A. Golbeck, Computing and applying trust in web-based social networks, University of Maryland, College Park, 2005.
[15] S.A. Kazmi, T.N. Dang, I. Yaqoob, A. Manzoor, R. Hussain, A. Khan, C.S. Hong, K. Salah, A novel contract theory-based incentive mechanism for cooperative task-offloading in electrical vehicular networks, IEEE Trans. Intell. Transp. Syst. 23 (7) (2021) 8380–8395.
[16] J. Kang, Z. Xiong, D. Niyato, D. Ye, D.I. Kim, J. Zhao, Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory, IEEE Trans. Veh. Technol. 68 (3) (2019) 2906–2920.
[17] X. Li, X. Li, H. Pan, "Multi-scale vehicle detection in high-resolution aerial images with context information," IEEE, Access 8 (2020) 208 643–208 657.
[18] J. Martínez-Cebrián, M.-Á. Fernández-Torres, F. Díaz-De-María, Interpretable global-local dynamics for the prediction of eye fixations in autonomous driving scenarios, IEEE Access 8 (2020) 217 068–217 085.
[19] D.T. Kanapram, F. Patrone, P. Marin-Plaza, M. Marchese, E.L. Bodanese, L. Marcenaro, D.M. Gómez, C. Regazzoni, Collective awareness for abnormality detection in connected autonomous vehicles, IEEE Internet of Things Journal 7 (5) (2020) 3774–3789.
[20] X. Liang, J. Zhang, L. Zhuo, Y. Li, Q. Tian, Small object detection in unmanned aerial vehicle images using feature fusion and scaling-based single shot detector with spatial context analysis, IEEE Trans. Circuits Syst. Video Technol. 30 (6) (2019) 1758–1770.
[21] J. Guo, A. Liu, K. Ota, M. Dong, X. Deng, N. Xiong, ITCN: an intelligent trust collaboration network system in iot, IEEE Transactions on Network Science and Engineering 9 (1) (2021) 203–218.
[22] C.C. Yen, D. Ghosal, M. Zhang, C.N. Chuah, Security vulnerabilities and protection algorithms for backpressure-based traffic signal control at an isolated intersection, IEEE Trans. Intell. Transp. Syst. 23 (7) (2021) 6406–6417.
[23] H. Xia, S.-S. Zhang, Y. Li, Z.-K. Pan, X. Peng, X.-Z. Cheng, An attack-resistant trust inference model for securing routing in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 68 (7) (2019) 7108–7120.
[24] C. Li, Y. Fu, F.R. Yu, T.H. Luan, Y. Zhang, Vehicle position correction: A vehicular blockchain networks-based gps error sharing framework, IEEE Trans. Intell. Transp. Syst. 22 (2) (2020) 898–912.
[25] K. Guo, Z. Wu, W. Wang, S. Ren, X. Zhou, T.R. Gadekallu, E. Luo, C. Liu, GRTR: Gradient rebalanced traffic sign recognition for autonomous vehicles, IEEE Trans. Autom. Sci. Eng. (2023).
[26] J. Kang, Z. Xiong, D. Niyato, S. Xie, J. Zhang, Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory, IEEE Internet of Things Journal 6 (6) (2019) 10 700–10 714.
[27] X. Xu, F. Wang, Trust-based collaborative filtering algorithm. 2012 Fifth International Symposium on Computational Intelligence and Design, IEEE, 2012, pp. 321–324.
[28] R. Xing, Z. Su, Q. Xu, N. Zhang, T.H. Luan, Secure content delivery for connected and autonomous trucks: A coalition formation game approach, IEEE Trans. Intell. Transp. Syst. 23 (11) (2022) 20 522–20 537.
[29] P. Kumar, R. Kumar, G.P. Gupta, R. Tripathi, BDEdge: Blockchain and deep-learning for secure edge-envisioned green CAVs, IEEE Trans. Green Commun. Network. 6 (3) (2022) 1330–1339.