Computers, Materials & Continua
DOI:10.32604/cmc.2021.017000
Article

Tech Science Press

Decision Making in Internet of Vehicles Using Pervasive Trusted Computing Scheme

Geetanjali Rathee[1], Razi Iqbal[2,*] and Adel Khelifi[3]

[1]Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan, 173234, Himachal Pradesh, India
[2]Department of Computer Information Systems, University of Fraser Valley, Canada
[3]Department of Computer Science and IT, Abu Dhabi University, United Arab Emirates, UAE
[*]Corresponding Author: Razi Iqbal. Email: razi.iqbal@ieee.org
Received: 18 January 2021; Accepted: 28 February 2021

Abstract: Pervasive schemes are the significant techniques that allow intelligent communication among the devices without any human intervention. Recently Internet of Vehicles (IoVs) has been introduced as one of the applications of pervasive computing that addresses the road safety challenges. Vehicles participating within the IoV are embedded with a wide range of sensors which operate in a real time environment to improve the road safety issues. Various mechanisms have been proposed which allow automatic actions based on uncertainty of sensory and managed data. Due to the lack of existing transportation integration schemes, IoV has not been completely explored by business organizations. In order to tackle this problem, we have proposed a novel trusted mechanism in IoV during communication, sensing, and record storing. Our proposed method uses trust based analysis and subjective logic functions with the aim of creating a trust environment for vehicles to communicate. In addition, the subjective logic function is integrated with multi-attribute SAW scheme to improve the decision metrics of authenticating nodes. The trust analysis depends on a variety of metrics to ensure an accurate identification of legitimate vehicles embedded with IoT devices ecosystem. The proposed scheme is determined and verified rigorously through various IoT devices and decision making metrics against a baseline solution. The simulation results show that the proposed scheme leads to 88% improvement in terms of better identification of legitimate nodes, road accidents and message alteration records during data transmission among vehicles as compared to the baseline approach.

Keywords: Pervasive computing; vehicular networks; security; trust; decision schemes; trusted internet of vehicles; big data

1 Introduction

Pervasive computing plays a significant role in resolving the issues of data processing in distributed heterogeneous environments. The involvement of various machine learning and IoT

devices allows automatic communication among the devices in real-time environment. Over the last few decades, a massive effort is being employed around the globe to introduce smart applications, including smart cities, smart homes, smart industries, smart grids, smart healthcare and smart transportation, to name a few [1,2]. The Internet and deployment of new technologies allow organizations and business players to communicate among each other. This pertains to the supply strategies, product suppliers, perspective and physical customers etc. In order to ensure an accurate, fast and immediate response, pervasive computing offers an excellent solution to various organizations and business perspectives. The term pervasive computing is defined as the use of automotive devices where number of objects share, access and process accurate and timely communications through various devices. It is a growing trend of computational capability where objects interact efficiently with the minimum or negligible involvement of the users. The devices are network-connected that interacts automatically from anywhere and at any time. Nowadays, industries are spending a lot of time and cost on research and development to explore various applications of pervasive computing. Because pervasive computing is capable of gathering, processing and exchanging information automatically, the technology can be adopted in variety of applications including activity and data context. IoV can be considered as a vital part of pervasive computing where the vehicles exchange or process the generated data through smart/intelligent devices. The pervasive IoV models can be further benefitted in reducing the traffic congestion, road accidents, weather forecasting and shortest route directions etc. From the user's perspective, pervasive computing is becoming a formidable solution in IoV to ensure an accurate and immediate vehicular communication as depicted in Fig. 1. The depicted Fig. 1 details the pervasive computing scheme in IoV having different types of processing methods such as integrating, transmission and analyzing over various vehicles. In addition, the subsection logic and decision making schemes are integrated to ensure a trusted and secure communication using several domain parameters over various attribute values. However, the number of security threats while computing or generating the pervasive decisions still reduces the business interest to fully adopt this technology. The IoV is a novel transportation technology or an application of pervasive computing where vehicles embedded with smart/intelligent sensors are connected to each other or with the adjacent infrastructure [3–5]. These vehicles collaborate with each other by sharing information such as accident warning etc. Furthermore, IoV is an emerging application of Intelligent Transportation System (ITS) which enables the users to make safer and better informed decisions by providing innovative services related to different modes of traffic management systems [6–9].

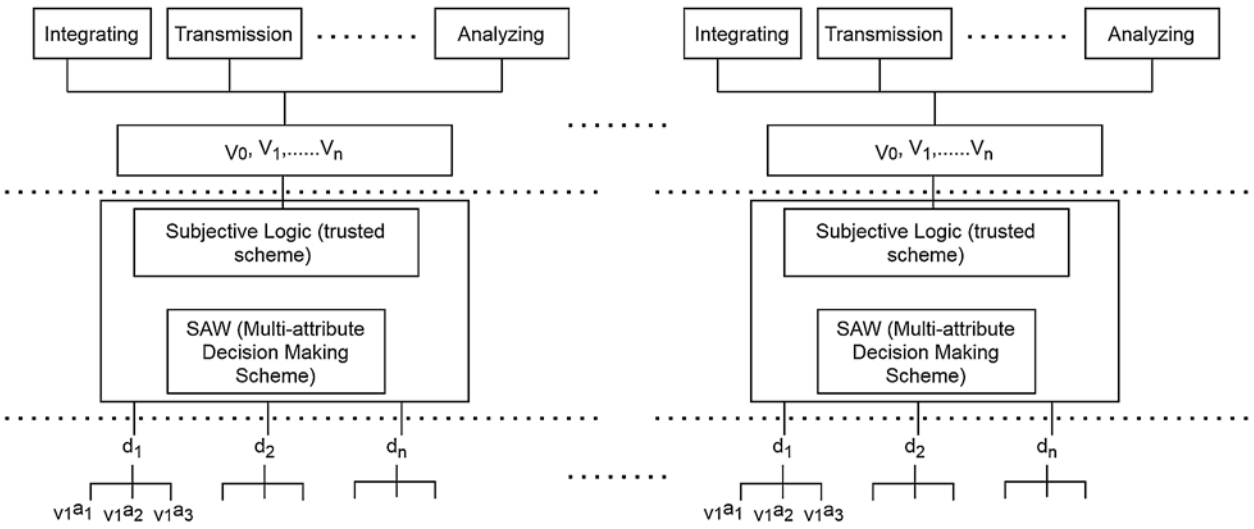

Figure 1: Pervasive computing in internet-of-vehicles

1.1 Motivation

The heterogeneity of various devices in pervasive computing makes IoV-enabled systems vulnerable to several security threats such as man-in-middle attack, denial-of-service attack, message alteration etc. In addition, the involvement of compromised devices while making pervasive decisions may involve various network degradation factors. The preservation of IoT objects from various security threats is also measured as a key issue along with the concern of revamping millions of daily life objects with latest technology which might not even get adapted as IoT devices. However, the goal to reduce environmental impact with the increasing number of vehicles on public roads evokes traffic safety concerns, which integrated with technological advancement leads to development and research in the area of cooperative and autonomous driving [10,11]. In addition, sovereign vehicles have the ability to improve the comfort for the drivers as well as passengers. Nevertheless, to bring automated vehicles in the market, we encounter substantial security issues that may only be conquered by critical research with insight along with driver support and local awareness by enabling pervasive vehicular systems. The main motive of autonomous driving is to perceive the environment with on board vehicle sensors, but due to high cost of sensors and their proximity limitations, sensors are only capable of detecting cooperative driving and line-of-sight objects. Platooning is considered as one of the popular vehicle to vehicle communication method where a vehicle follows the vehicle in its front by determining its distance and speed with its sensors [12,13]. In cooperative systems where sensors read data from other vehicles, it may also require certain methods to include those signals in their existing control systems for dealing with several security and complexity issues. Therefore, the main objective of this paper is to design a secure and trusted model using pervasive techniques for IoV.

1.2 Research Objective

By considering a variety of real-time applications of various smart devices, it is of utmost to secure the devices by preventing them from various intruders. Pervasive computing in the ITS environment transmit very sensitive information, such as the real time traffic monitoring, traffic congestion, weather conditions etc. Therefore, it must be a paramount necessity that security by design is provided to the automated network. Besides, the presence of malicious nodes may have severe impact on the automated network as they have the ability to tamper the data generated by the IoT devices [14,15]. Therefore, this leads to the question about how to provide a secure networking paradigm for enabling the devices to share data in an attack-free pervasive computing environment. In addition, the involvement of various security schemes may invade various security threats while making a real time decisions in the network. Therefore, we have considered the ITS application of IoV pervasive computing to highlight the need of security/trust during communication.

1.3 Contribution of the Paper

The aim of this paper is to introduce a trust system that examines real time traffic situations based on sensory readings and data from surrounding vehicles to guide decision making in automated and cooperative vehicles. The proposed mechanism is inspired by Xia et al. [16] where number of factors and attributes are considered to solve the trust of a sensor using decision making controller to provide safe and reliable decisions. In addition, for securing the communication among vehicles and devices, security schemes are foreseeable for pervasive computing vehicles. The proposed model has a system that supports real time decisions by indicating the trust in perceived situations. The potential contribution of the paper is further detailed as follows:

- A graph theory based trust factor mechanism is used to compute the authenticity of communicating vehicles in the network.
- Further, a multi-attribute scheme known as SAW method is applied to further improve the decision mechanism of the proposed ITS framework.
- The proposed scheme is analyzed over various simulating parameters such as trust nodes, record accuracy, DoS threat and detection rate security metrics.

The rest of the paper is structured as follows. Section 2 illustrates the related work in automated vehicular systems and the use of subjective logic and trust management system in ITS. Section 3 provides details of our proposed solution using subjective logic and trust methods to secure ITS networks. Next, Section 4 provides the details of the simulation model and the results and lastly, Section 5 concludes and directs the prospect of the paper.

2 Related Work

Variety of security schemes have been proposed by scientists and authors to include pervasive computing in ITS. This section describes various security mechanisms through several cryptographic, hypothetical, game theory and experimental methods to ensure security in pervasive computing ITS systems. Ivanov et al. [17] have presented a detailed discussion on vehicular to vehicular communication while exchanging the information among each other. They have illustrated the standardized mechanisms and cyber security threats such as ITU and ISO, ETSI and IEEE for enabling a security communication process in internet based vehicular systems. Tab. 1 determines the proposed mechanisms with their performance outcomes of various researchers/scientists. Rawat et al. [18] have proposed a data falsification detection approach in IoV using hash based scheme. The author's have used hash based encryption mechanism to enhance the vehicular communication mechanism by adopting accurate information about their neighboring environments. The authors have improved throughput and end-to-end delay using clustering scheme for reducing the traffic congestion.

Walker et al. [19] have determined an intrusion detection system within pervasive and ubiquitous environment to classify the threats both qualitatively and quantitative. The authors have examined the cyber security concerned in pervasive computing environment while processing the information through various smart/intelligent devices. Pei et al. [20] have proposed a secure pervasive edge computing model for IoV by designing a model having minimum system delay by considering the speed of vehicles. The sub-optimal and lower bound expressions are formed for allocating the power coefficients. Further, wold and frank algorithm is proposed to achieve an optimum power. Tithi et al. [21] have proposed a friendly jamming location verification security technique for vehicles in ITS to prevent eavesdropping attacks during communication among parties. In addition, the authors have presented an efficient distance bounding and friendly jamming method to detect any deviation and verify the velocity and location of vehicular infrastructure. The results analysis validated the realistic traffic using friendly jamming method with an improvement of 92% reduction rate against existing works. Passerone et al. [22] have addressed a secure pervasive computing issue among vehicles related to authorization and authentication of inter-vehicular safety commends. The authors have proposed a contract approach with the integration of arrowhead frameworks to ensure secure communication. The proposed mechanism is validated by representing the results on autonomous vehicles. The researchers are now days working on ITS deployment and development by addressing privacy and security concerns. In order to deploy successful communication among vehicles, it is needed that life-critical-safety concerns are not modified by the intruders. Panagiotopoulos et al. [23] have proposed a Diffie–Hellman vehicular

communication mechanism for authenticating the data in pervasive computing. The authors improved the security towards internet of vehicles system.

Table 1: Secure IoV mechanism proposed by various researchers

Author	Proposed scheme	Performance outcome
Ivanov et al. [17]	Vehicular to vehicular communication	They have illustrated the standardized mechanisms and cyber security threats such as ITU and ISO, ETSI and IEEE for enabling a security communication process in internet based vehicular systems
Rawat et al. [18]	Data falsification detection approach	The author's have used hash based encryption mechanism to enhance the vehicular communication mechanism by adopting accurate information about their neighboring environments
Walker et al. [19]	Intrusion detection system	The authors have examined the cyber security while processing the information through various smart/intelligent devices
Pei et al. [20]	Secure pervasive edge computing model	The proposed framework is simulated over minimum system delay by considering the various speed of vehicles
Tithi et al. [21]	Friendly jamming location verification	The results analysis validates the realistic traffic using friendly jamming method with an improvement of 92% reduction rate against existing works
Passerone et al. [22]	Secure pervasive computing	The proposed mechanism is validated by representing the results on autonomous vehicles
Panagiotopoulos et al. [23]	Diffie–Hellman vehicular communication	The authors improved the security towards internet of vehicles system
Cheon et al. [24]	Homomorphic cryptographic scheme	The proposed mechanism successfully enhances the security against forgery and eavesdropping attacks against computational tractability
Lai et al. [25]	Privacy and security scheme	The simulation and theoretical results indicate the optimal benefits in real time map updations to guarantee the reliability and efficiency of the pervasive vehicles
Dasjardins et al. [26]	Modern machine learning approach	The authors have used approximation function using gradient descent algorithm
Kang et al. [27]	Blockchain based mechanism	Hypothetical scenarios and probability methods have been proposed by the scientists

In order to enhance the security among automated vehicles such as channels, sensors and existing methods, various controlling systems are used. To protect the arithmetic operations of these controllers, Cheon et al. [24] have proposed homomorphic cryptographic scheme by proposing a linear homomorphic authentication encryption. The proposed mechanism successfully enhances the security against forgery and eavesdropping attacks against computational tractability. To further improve the road side accidents and safety, high precision maps can be used as additional information. Lai et al. [25] have proposed a privacy and security scheme for real time updates solving two issues i.e., completing quality and payment control systems. The authors have proposed a blockchain mechanism to protect the vehicles' privacy through blind signature

techniques. The simulation and theoretical results indicate the optimal benefits in real time map updations to guarantee the reliability and efficiency of the pervasive vehicles.

The improvements in communication, sensing and computations have led to the development of driver-assisted systems. In order to prevent from crashes and control the driver tasks, an adaptive cruise control mechanism was used to maintain the safety and security of the vehicles. Dasjardins et al. [26] have proposed a novel autonomous vehicle based on modern machine learning approaches. The authors presented the benefit of using reinforcement learning for secure longitudinal measures. The authors have used approximation function using gradient descent algorithm. In order to resolve this issue, Kang et al. [27] have ensured the security to the vehicles by proposing a Blockchain based mechanism. The proposed method verified the information using a two-level method i.e., data verification along with the selection of miner nodes. Also, the internal collaboration of each block is enhanced using content theory system where each and every block is verified by the miners.

Though a variety of security schemes in pervasive techniques based upon encryption algorithm, Blockchain mechanism, hypothetical scenarios and probability methods have been proposed by the scientists. However, each algorithm has its own security concerns such as computation delay, verification delay, key management overhead and so on. Further, the existing mechanisms have significant delay for validating the legitimacy of communicating device in real-time scenarios. In order to overcome from these issue, this paper has proposed a decision making scheme to ensure a secure IoV mechanism with reduced delay and overhead.

3 Proposed Mechanism

The trust among the communicating entities is defined to a significant factor to ensure a secure process in ITS mechanism. The involvement of trusted intermediate nodes during communication may reduce the efforts of computation process and delay in the network. Very few papers have introduced the concept of trust based security in ITS. This paper has proposed a trusted decision scheme while transmitting the message in ITS mechanism.

3.1 System Model

The system model of the proposed mechanism is shown in Fig. 2 and is based on graph theory consisting of vertices V, edges E, and Trust Factor (TF). The vertex V including $v_1, v_2, \ldots, v_n$, is the set of vertices that define the number of nodes in the network, E are the edges or links that establish a connection while sharing or transmitting the information in the network and e_{ij} is defined as a relation or a link from node v_i to v_j.

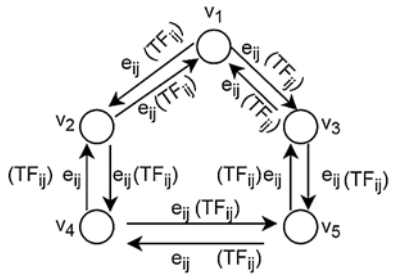

Figure 2: Identification of trusted IoT device

The links among nodes in the network may be direct (neighboring nodes that are directly attached) or indirect (nodes that are attached via more than 1 hop). Additionally, TF is a function as $TF : TF\left(e_{ij}\right) \rightarrow R\varepsilon(0,1)$ and represents a trust value that is a real number between 0 and 1 and between v_i and v_j. According to our proposed phenomenon, the trust model of IoV network is defined as a directed graph as shown in Fig. 2 consisting of five devices as $v_1, v_2, \ldots v_5$, with their edges e_{ij} and trust factor TF_{ij}. Now, the working of trusted pervasive mechanism using trust based factor is now detailed in below subsections.

3.2 Node's Trust Factor

The TF of each node in v_i and v_j is represented between 0 and 1 where 0 signifies an untrustworthy node while 1 implies a completely readable and trusted node. The trust grading criteria is depicted in Tab. 2 to determine the behavior of each node in the network. Further, a threshold value is assumed in order to differentiate between malicious and faulty nodes. If the TF of any device is less than 0.75 then it is regarded as a completely disinfected and malevolent node.

Now, the TF of the nodes in the directed graph are computed by analyzing their in-degree and out-degree where TF_{in} is defined as TF that the neighboring node gets about v_i while TF_{out} is the TF that v_i has about its neighbors.

Table 2: Definition of trust factor

Level	TF	Meaning
1	0, μ	Malicious
2	μ, 0.75	Faulty
3	0.75, 0.95	Trusted
4	0/95, 1	Complete ideal

3.3 Trust Classification

The trust values can be classified into three different types i.e., path information and historical information. Path trust value is defined as the value of a path from source to destination computed using TF_{in} and TF_{out} while the historical trust is the summation of multiple trust values such as recommended trust, direct trust, activeness and incentive function of each node.

Path trust on the other hand, is the one that determines the service levels based on the assessment of path TV. It can be determined as a constriction in routing decisions as $PTF_{ij} = \min\left(TF_{ik}\right)$ as shown in Fig. 2. PTF_{14} is defined as path 124 and is $i \leq k \leq j-1\, min\,(0.90, 0.86) = 0.86$.

3.4 Historical TF (HTF)

It is defined as a node's topological behavior based on historical information interaction computed by various decision factors such as recommended trust factor RTF_{ij}, Direct Trust Factor DTF_{ij}, Activation Trust Factor ATF_{ij} and Incentive Trust Factor ITF_{ij} that can be computed by Eq. (1).

$$HTF_{ij} = DTF_{ij} + RTF_{ij} + ATF_{ij} + ITF_{ij} \tag{1}$$

3.5 Recommending TF (RTF)

In order to fasten up the communication mechanism and reduce computational and communication overhead, the RTF_{ij} is used to predict the TF of the nodes that are repeatedly used while sharing or transmitting the information through a particular path in real time scenario. Initially, the threshold credibility of a recommended value is used to compared to the TF of a node. If the RTF_{ij} is greater than threshold, then we may use the recommended TF of that node. Recommended TF may use the RTF of that node. RTF may be for direct or indirect path recommended by only reliable and highly trusted nodes. $DTF = \min\left(TF_{ij}\right)$ while $ITF = min\sum T_{ik} + T_{kj}$.

3.6 Direct TF (DTF)

The direct path or link between two nodes is defined as a direct connection where the TF for direct link is called DTF. However, interaction among multiple hops and their information is defined as ITF. The direct TF_{ij} of a node v_i to node v_j is defined as the summation of t_{in} to v_j with total number of interactions as given in Eq. (2).

$$DTF = min\frac{TF_{ij}}{N_{tk}} \tag{2}$$

where k is the average of overall interaction computations within N intervals.

3.7 Activeness TF (ATF)

The malicious nodes in the network try to attract maximum number of nodes by specifying shortest path and a highly reliable behavior to trap ideal devices. The activation function is the degree through which the behavior of a number of nodes can be easily computed by analyzing their activeness in the network is defined as Eq. (3).

$$ATF = \frac{\mu}{I+1} \tag{3}$$

where I determines the cumulative entities that are associated with the node under evaluation v_j where μ is termed as threshold value.

3.8 Incentive Function (IF)

In order to encourage trustworthy nodes to participate in network communication and to generate an alarm upon identification of malicious neighboring nodes, the proposed framework has used an incentive function. An extra credit is assigned to each trusted node to find or inform any malicious node that is directly or indirectly connected to the network. Further, penalties are imposed on the nodes that act maliciously, the nodes having high penalty rates would be assigned a low TF and may be blocked permanently from future communication. The nodes having higher credit points are considered as highly trusted and can be used to recommend maximum number of neighboring nodes to fasten up their communication process as defined in Eqs. (4) and (5).

$$Trust\left(IF_i\right) = C_i\left(n\right) \quad and \tag{4}$$

$$Malicious\left(IF_j\right) = PR_i\left(n\right) \tag{5}$$

3.9 Subjective Adjective Weight (SAW)

Subjective Adjective Weight (SAW) [28] theory is a decision making model that is considered as one of the most significant multi criterion decision making schemes. SAW method integrates the quantitative and qualitative factors via multiple index assessment procedure in four different steps.

Step 1: Initially, generate an evaluation matrix consisting of M entities/node known as alternatives and N services. The first procedure of SAW is to create a decision matrix with the junction of each alternative and criteria. Now, let's denote $D = \left\{\left\{D_{i,j}\right\} : i = [1:n], j = [1:n]\right\}$ as the matrix of decision, where d_{ij} is the ith device rating with respect to the jth criteria.

Step 2: The generated matrix is normalized to r_{ij} by constructing a normalized matrix of decisions for beneficial and non beneficial attributes known as:

Beneficial attribute

$$r_{ij} = \frac{d_{ij}}{d_{ij}^{max}} \tag{6}$$

Non-Beneficial attribute

$$r_{ij} = \frac{d_{ij}^{max}}{d_{ij}} \tag{7}$$

Step 3: A weight set W_i for each $i = 1, 2 \ldots n$ is fixed for the service measures by creating weighted and normalized matrix of decision as:

$$V_{ij} = W_{ij} X_{ij} \tag{8}$$

where $\sum_{i=1}^{n} W_i = 1$

Step 4: The score of the ith alternative is computed by:

$$S_i = \sum_{j=1}^{m} V_{ij}, \quad i = 1, 2, 3 \ldots n \tag{9}$$

Step 5: At last, the Optimal Alternative (OA) is chosen as: $OA_{saw} = \sum_{i=1}^{n} S_i$ where S_i is the score metrics from alternatives score i.

We have used SAW to precisely determine the weight of trusted decision factors based upon nodes' historical behaviors as:

$$HTF_{ij} = W_1 RTF_{ij} + W_2 TF_{ij} + W_3 TF_{ij} \tag{10}$$

The execution of proposed mechanism is also described through an algorithm as mentioned in Algorithm 1.

Algorithm 1: Trusted algorithm (subjective logic and SAW)

Input: A set of 'n' devices/vehicles

Output: Device is trusted or malicious

Step 1: A network is represented through a directed graph having 'n' number of vertices 'V' $\epsilon v_1, v_2 \ldots v_n$ and 'n' number of edges 'E' $\epsilon e_1, e \ldots e_n$

Step 2: TF is computed by each node depending upon various criterions such as:

$$TF = RTF + DTF + ATF + ITF$$

Step 3: SAW approach is used to further to compute the TF to identify beneficial and non-beneficial attributes where,

(Continued).

$$\text{Beneficial attribute } r_{ij} = \frac{d_{ij}}{d_{ij}^{max}}$$

$$\text{Non-Beneficial attribute } r_{ij} = \frac{d_{ij}^{max}}{d_{ij}}$$

If $(device_{TF} > threshold)$ **then**
Device is trusted
Else
Device is malicious
End if

4 Performance Analysis

4.1 System State

The proposed trusted mechanism is analyzed using trust management system through SAW decision model against Kang et al framework. To validate and compare the results, the proposed approach is evaluated against number of networking metrics over existing method such as trusted nodes, data alteration, accuracy, satisfaction rate and etc. 200 nodes are initially deployed whose decision factors are updated after every 80 seconds. Further, the proposed approach's legitimacy is validated by intentionally adding malicious devices in the network. The simulation criteria used to determine the simulated results are represented in Tab. 3. Assumptions: Threshold value μ used to distinguish between types of devices is assumed as 0.49. The malicious nodes are increasing at 5% and 10% rate upon increasing the network size.

Table 3: Simulation parameters

S. No.	Parameters	Setting
1	Simulation area	400 m × 400 m
2	Number of devices	50
3	Vehicles mobility	0–5 m/s
4	Weight parameters	25, 45
5	Malicious rate	5%, 10%
6	Devices bandwidth	20 MHz

4.2 Existing (Conventional) Method

The efficiency and management of the proposed approach is evaluated using numerical simulations through MATLAB. Kang et al. [27] have ensured the security to the vehicles by proposing a Blockchain based mechanism. The proposed method verifies the information using two-level method as data verification along with the selection of miner nodes. Furthermore, the internal collaboration of each block is enhanced using content theory system where each and every block is verified by the miners. Incentive function, activation record and SAW approaches are used to analyze the trust of each communicating node. The SAW decision method is used to evoke the node's legitimacy by analyzing number of metrics using subjective logic function. The out performance of the proposed framework is verified against various security measures such as message alteration, node satisfaction, accuracy and detection of legitimate nodes.

4.3 Results and Discussion

The impacts of a trusted message system and SAW model while analyzing each and every activity of the IoV system are discussed in this paper. Fig. 3 depicts correct node identification based on the proposed approach. As clearly seen in the presented Fig. 3, the involvement of reputation model, incentive function and SAW function using multiple decision function ensures a better identification of communicating nodes (either malicious or trusted). However, existing (baseline) scheme performs less and exhibits reduced efficiency after increasing the intercommunication among IoT devices.

In addition, Fig. 4 represents record accuracy graph where upon increasing the number of nodes, it is very difficult to alter the transmitted or recorded data. The record accuracy of proposed phenomenon is better as compare to existing mechanism because of trust computation approach of each device while exchanging the information among each other.

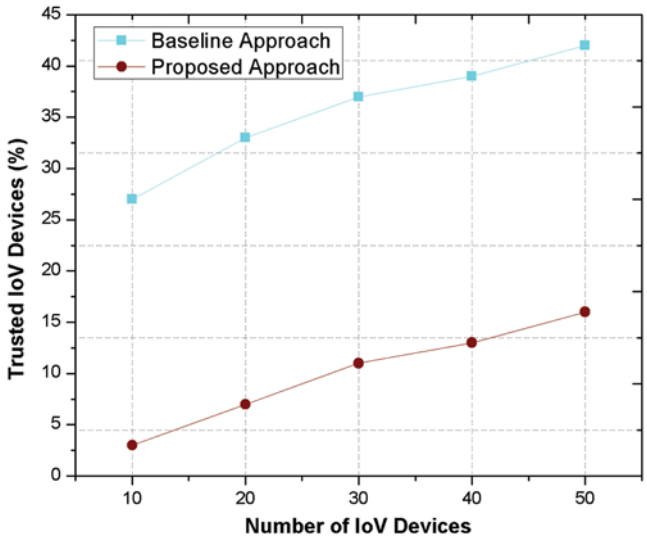

Figure 3: Identification of trusted IoT device

The incentive and activation functions adversely affect a node's reputation upon behaving maliciously and may possibly block or disown from communicating in the network. Subjective logic function efficiently analyzes the accuracy of communicating nodes by computing their trust values. However, the continuous analysis and recording of communicating nodes is very difficult in case of baseline mechanism. In addition, Fig. 5 determines the detection rate of malicious nodes using SAW approach. Subjective logic system filters out the overhead communication and networking congestion by computing non-beneficial and beneficial attributes. The filtered record management may speed up the computation process and identification of trust factors with more accuracy.

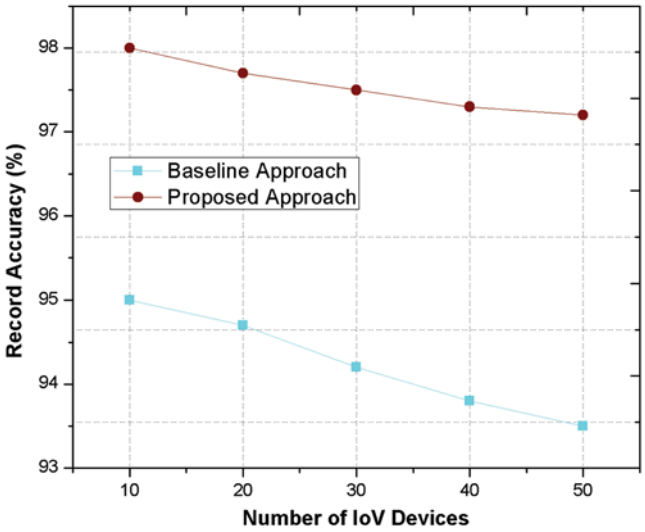

Figure 4: Record accuracy

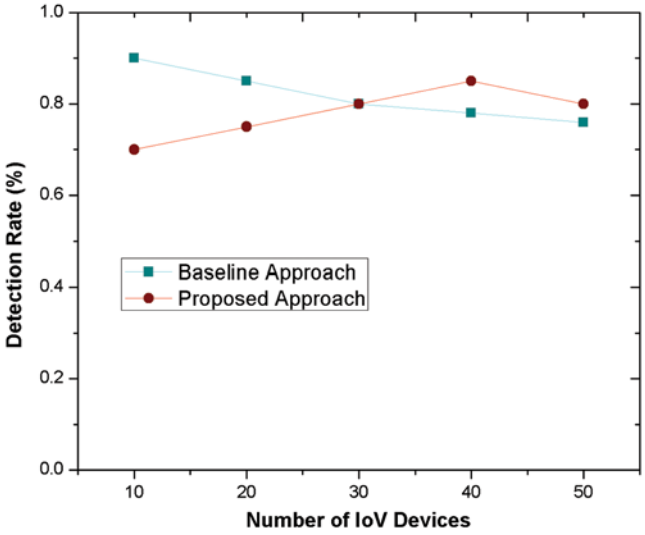

Figure 5: Detection rate

Finally, Fig. 6 evaluates the proposed scheme's out-performance against DoS malicious threat. During initial node's establishment where it is necessary to analyze node's authenticity, it may involve various malicious threats. The proposed approach outperforms as compare to existing mechanism because of involved pervasive techniques while communicating among various devices.

However, upon increasing the devices, proposed approach is successfully able to predict the malicious nodes performing various attacks in the network.

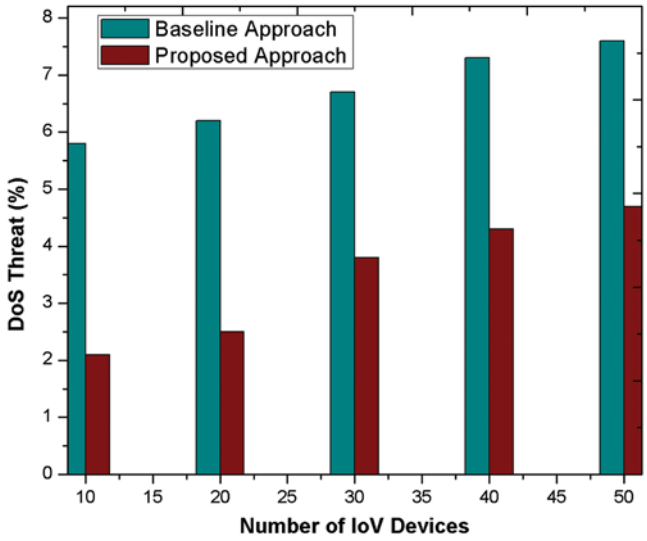

Figure 6: DoS detection threat

5 Conclusion

In this paper, we have considered an IoV application in pervasive computing to secure the process of data transfer in real-time environment. To further improve the safety and prevent road accidents and security issues, a variety of intelligent transportation systems have been proposed by various researchers. In this paper, a trusted security mechanism is proposed using various decision making factors and trust classification schemes. The proposed mechanism enhances the network security during pervasive computing where smart devices are generating and processing real time information without any involvement of human power. The proposed mechanism efficiently enhances the trusted node identification, record accuracy and detection rate using SAW approach having accurate and immediate identification of ideal communication nodes in the network. The results are simulated by analyzing the trust value of each device analyzing its communicational behavior. All the simulated results are verified over a conventional (baseline) approach. The number of patterns that can be further analyzed and learned by attackers still needs to be determined.

Further, how the proposed mechanism can be further improved having intelligent transportation scheme over dynamic attacking patterns with modified security threats may be considered in future work.

Acknowledgement: This work is supported by the Jaypee University of Information Technology, India, University of Fraser Valley, Canada and Abu Dhabi University, United Arab Emirates.

Funding Statement: The work was funded by the Abu Dhabi University, Faculty Research Incentive Grant (19300483–Adel Khelifi), United Arab Emirates. Link to Sponsor website: https://www.adu.ac.ae/research/research-at-adu/overview.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran *et al.,* "Internet-of-things-based smart cities: Recent advances and challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017.

[2] W. Zhang and X. Xi, "The innovation and development of internet of vehicles," *China Communications*, vol. 13, no. 5, pp. 122–127, 2016.

[3] F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, "An overview of internet of vehicles," *China Communications*, vol. 11, no. 10, pp. 1–15, 2014.

[4] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad *et al.,* "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[5] J. Zhang, F. Y. Wang, K. Wang, W. H. Lin, X. Xu *et al.,* "Data-driven intelligent transportation systems: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1624–1639, 2011.

[6] G. Rathee, A. Sharma, R. Kumar, F. Ahmad and R. Iqbal, "A trust management scheme to secure mobile information centric networks," *Elsevier Computers Communication Journal*, vol. 151, no. 1, pp. 66–75, 2019.

[7] M. H. Cintuglu, O. A. Mohammed, K. Akkaya and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446–464, 2016.

[8] R. Iqbal, T. Butt, M. Afzaal and K. Saleh, "Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions," *Sage International Journal of Distributed Sensor Networks*, vol. 15, no. 1, pp. 1–22, 2019.

[9] H. Sherazi, Z. Ashfaq, R. Iqbal, S. Rizwan, M. Imran *et al.,* "A Heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication," *Hindawi Mobile Information Systems*, vol. 19, no. 1, pp. 1–12, 2019.

[10] Y. Zhou, N. Cheng, N. Lu and X. S. Shen, "Multi-UAV-aided networks: Aerial-ground cooperative vehicular networking architecture," *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 36–44, 2015.

[11] N. Sumedh, M. S. Srinivasan, S. Basavaraju and N. Gangrade, "The MANI protocol for intra-vehicular networking," in *Smart Systems and IoT, Innovations in Computing*. Singapore: Springer, pp.63–74, 2020.

[12] H. Ghassemian, "A review of remote sensing image fusion methods," *Information Fusion*, vol. 32, no. 3, pp. 75–89, 2016.

[13] S. Li, H. Yin and L. Fang, "Remote sensing image fusion via sparse representations over learned dictionaries," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 51, no. 9, pp. 4779–4789, 2013.

[14] B. Mishra, P. Nayak, S. Behera and D. Jena, "Security in vehicular ad-hoc networks: a survey," in *Proc. of the 2011 Int. Conf. on Communication, Computing & Security*, Rourkela, Odisha, India, pp. 590–595, 2011.

[15] M. C. Chuang and J. F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE systems journal*, vol. 8, no. 3, pp. 749–758, 2013.

[16] H. Xia, Z. Jia, L. Ju, X. Li and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules," in *IEEE, 2011 IEEE/ACM Int. Conf. on Green Computing and Communication*, Chengdu, Sichuan, China, pp. 124–130, 2011.

[17] I. Ivanov, C. Maple, T. Watson and S. Lee, "Cyber security standards and issues in V2X communications for Internet of vehicles," *IET*, vol. 46, pp. 1–6, 2018.

[18] D. B. Rawat, M. Garuba, L. Chen and Q. Yang, "On the security of information dissemination in the Internet-of-Vehicles," *Tsinghua Science and Technology*, vol. 22, no. 4, pp. 437–445, 2017.

[19] J. J. Walker, T. Jones, M. Mortazavi and R. Blount, "Cyber security concerns for ubiquitous/pervasive computing environments," in *IEEE Int. Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Beijing, China, pp. 274–278, 2011.

[20] X. Pei, H. Yu, X. Wang, Y. Chen, M. Wen *et al.,* "NOMA-based pervasive edge computing: Secure power allocation for IoV," *IEEE Transactions on Industrial Informatics*, 2020. https://doi.org/10.1109/TII.2020.3001955 (Early Access).

[21] T. Tithi, B. Deka, R. M. Gerdes, C. Winstead, M. Li *et al.,* "Analysis of friendly jamming for secure location verification of vehicles for intelligent highways," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7437–7449, 2018.

[22] R. Passerone, D. Cancila, M. Albano, S. Mouelhi, S. Plosz *et al.,* "A methodology for the design of safety-compliant and secure communication of autonomous vehicles," *IEEE Access*, vol. 7, pp. 125022–125037, 2019.

[23] I. Panagiotopoulos and G. Dimitrakopoulos, "Diffie-Hellman process and its use in secure and authenticated VC networks," *IET Intelligent Transport Systems*, vol. 12, no. 9, pp. 1082–1087, 2018.

[24] J. H. Cheon, K. Han, S. M. Hong, H. J. Kim, J. Kim *et al.,* "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption," *IEEE Access*, vol. 6, pp. 24325–24339, 2017.

[25] C. Lai, M. Zhang, M. J. Cao and D. Zheng, "SPIR: A secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 416–428, 2019.

[26] C. Desjardins and B. Chaib-Draa, "Cooperative adaptive cruise control: A reinforcement learning approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1248–1260, 2019.

[27] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim *et al.,* "Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[28] W. Deni, O. Sudana and A. Sasmita, "Analysis and implementation fuzzy multi-attribute decision making SAW method for selection of high achieving students in faculty level," *International Journal of Computer Science Issues*, vol. 10, no. 1, pp. 671–674, 2013.