CRT-BIoV: A Cognitive Radio Technique for Blockchain-enabled Internet of Vehicles

Rathee, G., Ahmad, F., Kurugollu, F., Azad, M. A., Iqbal, R. & Imran, M.

Original citation & hyperlink:
Rathee, G, Ahmad, F, Kurugollu, F, Azad, MA, Iqbal, R & Imran, M 2020, 'CRT-BIoV: A Cognitive Radio Technique for Blockchain-enabled Internet of Vehicles', IEEE Transactions on Intelligent Transportation Systems, vol. (In-press), pp. (In-press).
https://dx.doi.org/10.1109/TITS.2020.3004718

DOI 10.1109/TITS.2020.3004718
ESSN 1524-9050

Publisher: Institute of Electrical and Electronics Engineers

CRT-BIoV: A Cognitive Radio Technique for Blockchain-enabled Internet of Vehicles

Geetanjali Rathee*, Farhan Ahmad†, Fatih Kurugollu†, Muhammad Ajmal Azad†, Razi Iqbal‡, Muhammad Imran§
*Department of Computer Science and Engineering, Jaypee University of Information Technology, India
†Cyber Security Research Group, College of Engineering and Technology, University of Derby, United Kingdom
‡Al-Khawarizmi Institute of Computer Science, University of Engineering and Technology, Lahore, Pakistan
§College of Computer and Information Sciences, King Saud University, Kingdom of Saudi Arabia
Email: *geetanjali.rathee123@gmail.com; †{f.ahmad, f.kurugollu, m.azad}@derby.ac.uk;
‡razi.iqbal@ieee.org; §dr.m.imran@ieee.org

***Abstract*—Cognitive Radio Network (CRN) is considered as a viable solution on Internet of Vehicle (IoV) where objects equipped with cognition make decisions intelligently through the understanding of both social and physical worlds. However, the spectrum availability and data sharing/transferring among vehicles are critical improving services and driving safety metrics where the presence of Malicious Devices (MD) further degrade the network performance. Recently, a blockchain technique in CRN-based IoV has been introduced to prevent data alteration from these MD and allowing the vehicles to track both legal and illegal activities in the network. In this paper, we provide the security to IoV during spectrum sensing and information transmission using CRN by sensing the channels through a decision-making technique known as *Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS)*, a technique that evokes the trust of its Cognitive Users (CU) by analyzing certain predefined attributes. Further, blockchain is maintained in the network to trace every activity of stored information. The proposed mechanism is validated rigorously against several security metrics using various spectrum sensing and security parameters against a baseline solution in IoV. Extensive simulations suggest that our proposed mechanism is approximately 70% more efficient in terms of malicious nodes identification and DoS threat against the baseline mechanism.**

***Keywords*—Internet-of-Vehicles, Cognitive Radios, Blockchain, TOPSIS, Spectrum availability**

I. Introduction

With the continuous development of wireless technologies in the transportation industry, Vehicular ad-hoc networks (VANET) have emerged as a promising research area consisting of a group of stationary and moving vehicles controlled via automated and embedded systems. It is estimated that there will be more than 250 million connected vehicles by the year 2020 [1]–[3]. Until recent times, the main aim of VANET was to provide comfort and safety to drivers in a vehicular environment by collecting and sharing data with other drivers [4]–[6]. However, VANET is transforming rapidly towards a transportation system where smart vehicles equipped with embedded sensors, adapters and controlling units can not only monitor their surroundings but also effectively communicate with neighboring vehicles. This results in a novel paradigm known as "Internet-of-Vehicles" (IoV) where vehicles can share the information with neighboring vehicles in an efficient manner. Further, IoV provides Internet connectivity to the vehicles, thus providing improved data sharing in the form of risk, sensory and data localization through on-board connected smart devices [7]–[9].

Recently, with the continuous increase in urban population and rapid expansion of cities, automated machines are fast entering every sphere of life where device ownership has been controlled via Internet of Things (IoT) devices [10]–[14].

In addition, the evolution of technologies where smart devices automate the environment has led to several security and bandwidth availability issues such as spectrum range, data bandwidth support, and spectrum availability. Further, with the use of smart technologies, the IoT applications can be altered by the malicious intruders where a massive amount of data is injected into the network which further escalates the issue of handling spectrum scarcity [15]. Recent trends of research in Cognitive Radio Networks (CRNs) have drawn potential attention to solve the above-mentioned issues [16], [17]. CRN is an intelligent wireless communication system that is aware of its environment with two primary objectives, namely (1) highly reliable communication whenever and wherever needed, and (2) efficient utilization of radio spectrum.

A. Research Objective

1) Need for CRN in IoV: One major drawback of IoV is sensing spectrum availability and sharing/transferring a large volume of data from many meters/devices in a limited spectrum bandwidth without interference to long distances. Current wired technologies require DSL and optical fiber cables to ensure communication among base stations. Further, the use of wired communications require huge expenditures for cable/fiber installation or spectrum purchase. Therefore, we are left with CRNs as a viable solution in IoV where objects are equipped with cognition in order to learn, think and make decisions through understanding of both social and physical worlds [18], [19]. Further, additional requirements such as intelligent decision making, perception-action cycle, massive data analytics, on-demand service provisioning, semantic derivation, and knowledge discovery also encourage the combination of IoV with CRNs to take correct decisions in case of threat encounter. In case where intruders try to hack the vehicles (devices), the cognitive-based IoV system may help

to further enhance the security by taking intelligent decisions of blocking or punishing the malicious objects. Therefore, a CR-based IoV is a foreseeable need in the future due to the following reasons.

- CRNs perceive the spectrum environment and provide on-demand services to the users through intelligent decision making.
- The IoV objects equipped with cognitive capability can achieve seamless connectivity and resolve the issue of channel unavailability for online data sharing.

However, in spite of a lot of advantages, the CRN-IoV may also lead to several security and networking issues. In this paper, we highlight the issues of spectrum sensing and data sharing among available vehicles during mobility. Generally, in CRN-IoV a security breach can occur during both the processes, namely, 1) data sharing, wherein a centralized infrastructure, intruders may sabotage a single point to breach the entire security [20], [21]. On the other hand, the decentralized infrastructure leads to access to data without security and authorization. 2) A spectrum sensing, where traditionally, all the Cognitive Users (CUs) are often assumed to be trusted and cooperative. However, in practice, the CUs which sense the availability of empty bands or transfer huge amount of data to FC (Fusion center) can be compromised by the intruders to introduce malicious attacks by submitting false reports to FC or manipulating the data for their own means. The compromised IoT based CU behaves as a Malicious User (MU) which mostly forwards untrusted sensing reports to the network [16], [22].

Further, the transmission of untrusted sensing reports to the FCs or CRNs may lead to an increase in the congestion, excessive consumption of network resources, exploitation of nodes' energy and so on. Thus, the potential challenge with CRN-IoV is to evolve it into a trusted sensing technique that can efficiently distinguish legitimate CUs from MUs.

2) Need of Blockchain in CRN-IoV: Recently, Blockchain is considered as an emergent security technique which provides an efficient and transparent mechanism for analyzing and controlling the data [23], [24]. Several researchers have proposed various blockchain solution in IoV [25], [26] in order to maintain transparency during data transfer/sharing in IoV. The blockchain technique in CRN-IoV has been introduced that not only ensures security but also provides traceability of IoT devices or vehicles to trace legal or illegal activities [27], [28]. Besides, with the increasing number of technologies, there is a need to provide spectrum availability to the devices that generate a huge amount of data and ensure secure sensing of vacant bands and data sharing in real time scenarios. For ensuring secure sensing and data sharing processes, transparency and security can be easily provided by Blockchain mechanism that records each and every activity of communicating entities. A single alteration in data or false sensing reports by a malicious entity can be easily traced by the remaining smart (cognitive) devices who are the part of a blockchain network. Also, the security concerns such as centralized failure system, data authorization during data sharing among IoV can be easily resolved using Blockchain mechanism [29], [30]. Therefore, Blockchain can be considered as a viable security solution in IoV using CRN.

Further, in order to limit the storage of duplicated information captured by IoT devices in continues manner and to overcome the storage and computational overhead issues in Blockchain mechanism, various data filtering schemes may be used to get/store the data on a blockchain after a specific interval of time. A data controller manager at the IoT network may receives the information that filter out the specific information to be stored at the blockchain. In order to understand it in a better way let us consider an example where IoT devices continuously captures the data of product manufacturing of an industry. The IoT devices will capture each and every detail of product such as product name, product id, quality, price, manufacturing time, date, amount and so on. Now, controller manager will filter out specific information such as product id recorded by specific IoT device after a specific interval of time and then store this single information into the blockchain to further filter out the complexity and storage overhead. The filtering process of information and storage of record after a specific interval of time by any controller (manager) may limit the size of data stored in the blockchain and reduce the storage overheads and complexity in the network.

B. Paper Contribution

In this paper, we have provided the security to IoV during spectrum sensing and information transmission process using CRN by sensing the channels through a decision making technique known as the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [31]. TOPSIS is a multi-structured selection technique that appoints the trust to its CUs by analyzing certain attributes including transmission time, energy consumption and interaction effects. Any change in sensing reports or information provided by smart devices may be reflected in the FC. Further, a Blockchain mechanism has been used to maintain transparency among the vehicles during data sharing. The experimental data of the proposed framework has been analyzed against the illegal activities or communications carried out by malevolent IoT objects where the percentage of secure vehicular data upon compromising of IoT devices has been discussed against various security metrics [32], [33]. Therefore, in this paper, an attempt has been made to design a trust evaluation framework that uses a trust manager (TOPSIS) to evaluate the trustworthiness of CUs. The proposed framework employs TOPSIS to compute trustworthiness of IoT devices by monitoring the services provided by them by addressing the issue of selection of trustworthy CU using a decision making strategy.

he integration of the Blockchain mechanism in IoV has attracted the attention of developers and scientists because of its anonymity, decentralized and trusted intelligent ecosystem. Though researchers have proposed various Blockchain schemes, however, existing schemes have not sufficiently addressed the data-sharing issues in IoV. The proposed mechanism incorporates the Blockchain network to ensure a secure and transparent data transferring in the IoV. The proposed mechanism is ensuring the security to IoV at two levels:

- *Security using a decision-making process*: TOPSIS is used to legitimate CUs so that FC can find the correct sensing report managing the availability of channels, transfer of data over the Internet, etc.
- *Security using blockchain:* The blockchain mechanism is used to keep the chain of blocks which hold the data in IoV. Further, the voting miners keep the same chain and verify or validate the newly entered vehicles.

C. Outline

The remaining structure of the paper is organized as follows. The related works of CRN-IoV and blockchain are presented in Section II. The hybrid Blockchain technology using TOPSIS method is described in Section III. Further, Section IV illustrates the performance analysis of the proposed framework. Finally, Section V concludes the paper and highlights the future scope.

II. Related Work

The involvement of an intelligent wireless communication system that ensures reliable communication whenever and wherever needed leads to efficient utilization of the radio spectrum. This section discusses the need for IoT based cognitive radio networks in IoV applications. Awin et al. [34] have discussed a survey focused on cognitive radio-based IoT frameworks by illustrating efficient sensing and sharing of spectrum bands. The authors have illustrated the benefits and drawbacks of the sensing and sharing spectrum by discussing the criteria and designing factors of CR-IoT along with suggesting open issues and future directions. However, the need for security and privacy concerns while sensing the bands are missing in this paper. Further, Xia et al. [35] have inspected the Q-learning based power control strategy of intelligent secure communication with statistic state information for IoT. The authors have analyzed the security patterns of attacks in terms of jamming, silent, spoofing and eavesdropping. Further, the simulated results presented the impact of the attacker's channel state information and concluded the security performance in terms of launching an attack and the cost of an intruder. Moreover, the proposed approach is evaluated against instantaneous channel state information in terms of security. However, the intruders may still able to perform various attacks by learning and recognizing the defense patterns in the network. Wen et al. [36] have proposed a centralized cooperative CRN where the cognitive user transmitter behaves like a friendly jammer which does not submit the honest report due to its mischievous reasons. To overcome this issue, the mechanism computed the trust degree of each cognitive user transmitter in the statistical and perfect channel state information. The authors have analyzed the degree of trust and trust list using a threshold of each cognitive user transmitter for both the cases. However, the attacks can be further performed by analyzing the attacking patterns.

Several authors have studied the CRN applications in IoV using 75 MHz to increase spectrum opportunities with an increased number of connected devices. Eze et al. [21] have proposed a CR assisted vehicular network that encourages CR enabled devices to use licensed spectrums. Also, authors have proposed a three-stage spectrum allocation and sensing model by applying the optimal sensing algorithm to guarantee the secured acquisition of channels within sensing time. The proposed mechanism is simulated and theoretically analyzed with improved cooperative sensing and spectrum opportunities to vehicles. However, there is a need to propose an efficient and novel cognitive technique to resolve spectrum scarcity and spectrum management issues with the increased demand on vehicular applications. Further, Qian et al. [37] have modeled 0-1 programming known as a convex optimization problem for path selection of switches. The optimization problem is again converted into log-det heuristic algorithms with the lowest delay and security requirements. The proposed mechanism is validated against other schemes through an experiment. However, the increasing number of devices may further degrade security while communicating in the network. Paul et al. [38] have proposed an efficient centralized and distributed cooperative sensing in vehicular networks. The proposed model is analyzed over decision fusion schemes using renewal theory by analyzing the probability of primary channel detection and average time. Also, a mathematical analysis is formulated to verify the false alarm and probability of detection. The results showed that the proposed scheme is more suitable against interference minimization and the hidden problem of Primary User (PU). Further, Hu et al. [39] pointed out the issue of secure communication and nodes authentication in IoV for intelligent transportation. By considering the issues of complexity and centralized mechanism in IoV, authors have integrated the blockchain in IoV to generate a decentralized communication. In the proposed blockchain architecture, authors have used a gossip protocol and byzantine algorithm to complete consensus authentication and communication. The proposed mechanism also ensured fault tolerance during the communication mechanism. The simulated results validated the performance of the proposed mechanism against consensus and information security efficiency. However, the authors have not highlighted the need for a blockchain mechanism in cognitive radio.

Data sharing is becoming critical for improving the services and safety of vehicular networks. Even though authors have proposed various blockchain schemes to ensure transparency during data sharing, however, the selection of miners may collide among compromised and legal candidates. In order to resolve this issue, Kang et al. [40] have proposed a two-stage security enhancement scheme for block verification and miners selection. Initially, a reputation based scheme is used to ensure miners selection that evaluates the reputation based on past and recommended opinions of neighbouring nodes. Further, a content theory model is used to verify the newly generated block that avoids the internal collusion among miners. The simulated result verified the efficiency and security of data sharing in IoV using blockchain. However, the two process mechanism further increase the communication and computation overhead in the network. Rahman et al. [41] have proposed a blockchain-based framework to ensure the privacy and security of Spatio-temporal contract services for IoT in smart cities. The proposed mechanism influences cognitive fog

nodes to process multimedia transactions and payload from IoT and mobile edge nodes using artificial intelligence that extracts and processes event information. Further, to assist the sharing services, the results are stored in decentralized clouds and blockchain networks. However, the authors have not discussed the issue of secure sensing to identify the legitimate vacant channel. Though, authors have proposed various security mechanisms based on cognitive networks in IoV [42], [43]. However, there are still some key open research challenges to be addressed:

- In the multi-hop CR scenario, there is a need to address the issue of spectrum sensing. In this context, the exposed or false submitted sensing reports to FC needs to be resolved.
- Most of the works use simple ON/OFF models for PU activities. However, in reality, there are many types of PUs due to heterogeneous networks that need to be considered.
- After sensing procedures, the IoT assignment policy of radio resources needs to be efficiently performed.

In the next section, we show how multi decision paradigm and the CR blockchain technology cooperation can solve the above-mentioned issues.

III. Proposed Solution

The proposed CR blockchain mechanism for secure IoV is distributed in two subsections 1) spectrum sensing using TOPSIS and 2) data sharing through blockchain. Table I provides the list of notation used in this paper.

TABLE I: Abbreviations List

Terms	Meaning
IoT	Internet of Things
IoV	Internet of Vehicles
CRN	Cognitive Radio Network
PIS	Positive Ideal Solution
NIS	Negative Ideal Solution
CU_{ij}	Matrix of i,j Cognitive User
N_k	Number of devices interacting with each other
VANET	Vehicular Ad-hoc Networks
FC	Fusion Centre
TM	Trust Manager
OMV	Overall Measured Value
CMV	Current Measured Value
RC_i	Relative Closeness of i_{th} CU
RF_i	Relative Fairness of i_{th} CU
CP_i	Cognitive Parameters of i_{th} CU
NCP_i	Normalized Cognitive Parameters of i_{th} CU
$d_{i,j}$	Interaction of device i to device j
P_i	i number of trust measuring parameters
$t_{i,j}$	Euclidean distance of CU_i from CU_j
A_I	Ideal Alternative
A_N	Non-ideal Alternative
S_{i-}	Distance of alternative i from NIS
S_{i+}	Distance of alternative i from PIS

A. Spectrum sensing using TOPSIS

In order to describe our proposed solution, we need to introduce the secure sensing mechanism where IoT based cognitive users sense the availability of free bands and submit their reports to the Fusion centre (FC). FC is a centralized framework that conducts an independent assessment of CUs' performance, analyze the security and availability of ideal channels. For sensing and analyzing available spectrum bands, CUs are equipped with intelligent sensors. Besides, a trusted method (TOPSIS), where the CUs' trust is measured by FC through intelligent sensors to compute the legitimacy during submission of their sensing reports, is adopted. Further, FC evaluates the submitted reports and analyze the services (features) provided by CU in terms of channel availability, security and privacy measures. The proposed framework employs TOPSIS in FC to evaluate the trustworthiness of CUs.

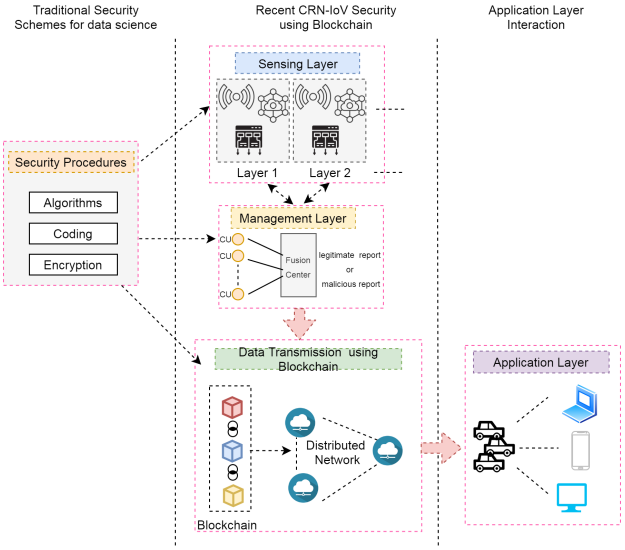

Fig. 1: CRN-IoV using Blockchain

Table II describes major entities of the proposed mechanism and Figure 1 depicts the CRN-IoV framework where there is a need for secure communication and transferring of information through legitimate CUs in real-time scenarios. Further, the Trust Manager (TM) or TOPSIS method is engaged by FC for monitoring the submitted sensing reports by certain measuring parameters. The parameters are monitored and the trust is evaluated with respect to the finalized report of FC. Performance evaluation and monitoring related reports, that are stored and managed by FC, are generated in specific intervals of time during the sensing phase. Further, alarms are triggered if the monitored trust value is found to be extremely low. The next section describes the security measuring parameters that can be used for performance monitoring in CRN-IoT.

1) Parameters for performance monitoring and trust evaluation of sensing reports: A variety of computation and service parameters are defined in the studies for performance monitoring. Interaction frequency, energy consumption, interaction timeless, transmission time and interaction effects are various parameters that are considered while evaluating the results.

- *Interaction frequency:* Number of devices interacting with each other to the average number of times the devices interact.

$$Interaction_{d_{i,j}} = \frac{d_{i,j}}{\sum N_k} \tag{1}$$

where k=1,2,...n

TABLE II: Proposed Entities of the Framework

Entity	Details
FC	Responsible to collect sensing reports from different CUs and analyze legitimate and malicious reports generated by trusted/malicious users
CU	Responsible to identify/vacant bands for communication and data sharing mechanisms
TM (TOPSIS)	Used to compute trust of each vehicle and identify legitimate and trusted CUs
IoT devices	Responsible to collect and provide information requested by vehicles during mobility

- *Energy consumption (EC):* Energy consumed by each device while transmitting the data or communicating with each other (This energy is proportional to the amount of data sent and received).

$$EC_{node} = data\ receiving + data\ forwarding \quad (2)$$

- *Interaction timeless:* In IoV, sensors are not always reliable and trusted because of a lack of security and privacy protections. The recent and past interactions have a huge impact on the local opinions of sensors. The interaction rate is defined as the ratio of interactions among legitimate devices and malicious, legitimate devices.

$$Interaction_T = \frac{legitimate}{malicious + legitimate} \quad (3)$$

- *Transmission time:* Amount of time required to respond to the requesting user.
- *Interaction effects:* The positive and negative interactions by legitimate or malicious devices during transmission or communication among each other.

$$Interaction_E = \frac{+ve\ interaction\ by\ LN}{+ve + -ve\ by\ (MN + LN)} \quad (4)$$

where, LN is the legitimate node and MN is malicious node.

During the performance measurement, the above mentioned computation and service parameters are considered. These parameters may be monitored several times during a given/fixed time interval. If $OMV_{p_i}^{t-1}$ represents the Overall Measured Value (OMV) of parameters P_i at time $t-1$, then the OMV of parameter P_i at time t (expressed as $OMV_{p_i}^{t}$) is computed as:

$$OMV_{p_i}^{t} = \frac{OMV_{p_i}^{t-1} + CMV_{p_i}^{t}}{n_{p_i}^{t-1} + 1}, \quad (5)$$

where $OMV_{p_i}^{t}$ is measured value of parameter P_i at time t, $CMV_{p_i}^{t}$ is the current measured value of parameter p_i at time t and $n_{p_i}^{t-1}$ is the number of values measured for parameter P_i till time $t-1$. For trust evaluation, the OMV of parameter $P_i(OMV_{p_i}^{t})$ is compared with the actual values offered by CU. The compliance of parameter P_i at time t, expressed as $C_{p_i}^{t}$, is calculated as:

$$C_{p_i}^{t} = \frac{OMV_{p_i}^{t}}{FC_{p_i}}, \quad (6)$$

Where CU_{p_i} is the value offered by CU for parameter P_i as per FC. Next section explains how trust values of various parameters are used to evaluate the trustworthiness of CU's.

2) Fusion centre trust evaluation process: The process of analyzing the trust and security measures can be articulated as a decision-making model. This model can be represented hierarchically as shown in Figure 2 consisting of TOPSIS and Blockchain framework. TOPSIS is used to identify the behavior of each device (malicious or legitimate) while Blockchain framework is used to maintain transparency among the devices while sharing data. These kinds of problems have been defined in the literature as multiple criteria decision-making problems. Suppose you want to buy a car having various types of models and styles and your motive is to purchase the best model. Thus, the task of decision-making problem is to rank the various features of the criteria of a car based on their model. Therefore, decision-making problem involves managing trade-offs or compromises among various categories that conflict with each other.

The TOPSIS method was developed by Hwang and Yoon [44]. This method is based upon the concept that the chosen alternative should have the shortest Euclidean distance from an ideal solution and farthest from the negative ideal solution. The ideal solution is a hypothetical solution for which all attribute values correspond to maximum attribute value in the database comprising the satisfying solutions; the negative ideal solution is the hypothetical solution for which all attribute values correspond to the minimum attribute value in the database. The main procedure called TOPSIS which is employed by FC is as follows:

1) Construct an evaluation matrix consisting of n CUs (alternative) and m security parameters with the intersection of each alternative and criteria given as $CU_{(i,j)}$, where $i = 1 \ldots n$ and $j = 1, 2, \ldots . m$. Therefore, we have a matrix $M(CU_{n \times m})$. In this matrix, $CU_1, CU_2 \ldots\ldots\ldots CU_n$ are the n sensing parameters, $CP_1, CP_2, \ldots\ldots CP_m$ denote the trust levels of m parameters (Cognitive Parameters) and $CU_{i,j}$ represents the compliance level of j^{th} parameter of i^{th} CU.
2) The matrix $CU_{(n \times m)}$ is normalized to form the matrix $NCU_{(n \times m)}$. The values in this matrix range from 0 to 1, where 1 is the most complaint parameter of sensing while 0 is the least complaint parameter of the computation. $NCU = CU_{n \times m}$, using the normalized method.
3) A set of weights w_j (for j=1,2,....m) such that $\sum w_j = 1$ have to be decided for sensing parameters. Parameters are interaction frequency, timeliness, effects, energy consumption, transmission time to measure the legitimacy of a node. However, weight is further assigned to each node by measuring certain parameters.

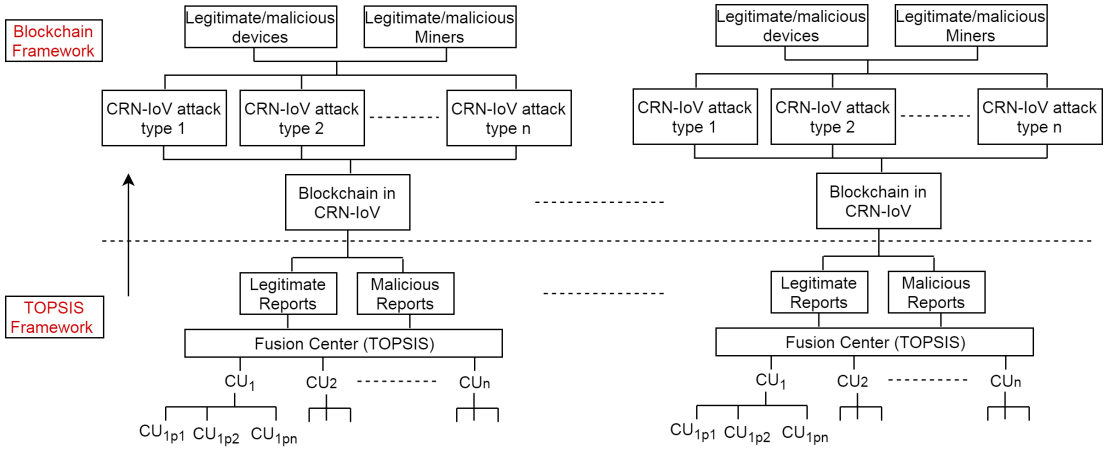

Fig. 2: Hierarchical model

$$P_{n\times m} = \begin{matrix} Parameter \\ P_1 \\ P_2 \\ \vdots \\ P_n \end{matrix} \begin{bmatrix} P_1 & P_2 & \dots & \dots & P_n \\ 1 & P_{12} & \dots & \dots & P_{1n} \\ P_{21} & 1 & \dots & \dots & P_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ P_{n1} & P_{n2} & \dots & \dots & 1 \end{bmatrix} \quad (7)$$

4) Calculate the weighted normalized decision matrix of each CU corresponding to each parameter.

$$T = (t_{m\times n}) = (w_j NCUWP_{i,j})_{m\times n} \quad (8)$$

where i=1,2,....m, j=1,2,....n and $NCUWP_{(i,j)}$ is normalized CU weighted which is obtained after various calculated parameters.

5) Determine the ideal alternative A_i and non ideal alternative A_N for every QoS parameter carried out in 8). Calculate the weighted normalized decision matrix by employing perspective weights PW_j from Step 5.

$$T = (t_{m*n}) = (PW_j NCP_{i,j})_{m*n}, \quad (9)$$

where i=1,2,....m and j=1,2,....n and NCP is (Normalized Cognitive Parameters)

6) Determine the Ideal alternative (A_I) and the Non Ideal alternative (A_N) for each perspective (legitimate and malicious).

$$A_I = \begin{Bmatrix} \langle min(t_{ij}|i = 1,2,..,m)|j \in J_- \rangle \\ \langle max(t_{ij}|i = 1,2,..,m)|j \in J_+ \rangle \end{Bmatrix} \equiv \left\{ t_{Ij} = 1,2,\dots,n \right\} \quad (10)$$

$$A_N = \begin{Bmatrix} \langle max(t_{ij}|i = 1,2,..,m)|j \in J_- \rangle \\ \langle min(t_{ij}|i = 1,2,..,m)|j \in J_+ \rangle \end{Bmatrix} \equiv \left\{ t_{Nj} = 1,2,\dots,n \right\} \quad (11)$$

where

$$J_+ = \left\{ j = i = 1,2,..,n| \right\}$$

where, j associated with the criteria having a positive impact and

$$J_- = \left\{ j = i = 1,2,..,n| \right\}$$

where, j associated with the criteria having a negative impact

7) Obtain separation measures. The separation of each alternative from the ideal one is given by the Euclidean distance in the following equations:

$$S_{i+} = \left\{ \sum_{j=1}^{n} (t_{ij} - t_{Ij})^2 \right\}^{0.5} \quad (12)$$

$$S_{i-} = \left\{ \sum_{j=1}^{n} (t_{ij} - t_{Nj})^2 \right\}^{0.5} \quad (13)$$

In above equations, i=1,2,....m and j=1,2,....n

8) The Relative Closeness (RC) of a particular alternative to the ideal solution is specified as RC_i which is expressed in this step as follows:

$$RC_i = \frac{S_{i-}}{(S_{i+} + S_{i-})} \quad (14)$$

where i = 1,2,..,m. From RC_i, Relative Fairness (RF_i) is derived as RF_i = 1 - RC_i.

9) Obtain variance from NCP_{ij} for each $CP_i = 1,2,..,m$ expressed as $V_i = variance(NCP_{ij})$, where $j = 1,2,..,n$.

10) Obtain final trustworthiness FT_i, final untrustworthiness FUT_i, and final uncertainty FU_i for CP_i from RC_i, RF_i, and V_i as:

$$FT_i = \frac{RC_i}{RC_i + RF_i + V_i} \quad (15)$$

$$FUT_i = \frac{RF_i}{RC_i + RF_i + V_i} \quad (16)$$

$$FU_i = \frac{V_i}{RC_i + RF_i + V_i} \quad (17)$$

11) Rank the alternatives according to $FT_i, i = 1, 2, .., m$, where Final Trustworthiness rank of i^{th} CU.

The procedure outlined above is the logic to evaluate final trustworthiness by considering a different number of perspectives. The legitimacy of each CU is calculated using RC and RF to further analyze their communication behaviour. Further, TOPSIS method is used to categorize the behavior of each device depending upon its communication in the network. In order to reduce the computation overhead, the attributes are divided into two different types i.e. ideal and non-ideal (as shown in equation 10 and 11). The ideal attributes are the one that directly affects the trust of a device to compute its legitimacy while non-ideal attributes are the indirect ones that may or may not adversely affect the device behavior. The proposed phenomenon considered ideal attributes during simulation analyses to reduce the computation overhead and accurately analyze the behavior of each node.

B. Data Sharing through Blockchain

The blockchain technology can build control systems and data sharing systems for CU in order to address the challenges of decentralized information circulation, internal information controlling access and privacy while sharing the data among various entities. Figure 3 depicts the data-sharing mechanism through blockchain where each record of every individual entity is stored on a blockchain network that can be further traced and analyzed by all the users. The malicious data record or alteration in stored information can be immediately identified by all the entities (CU).

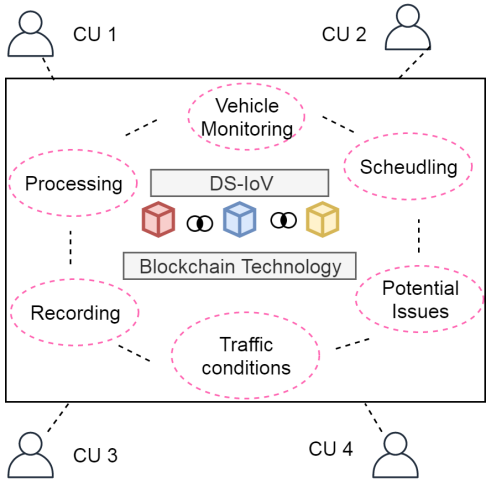

Fig. 3: Hierarchical model

Though TOPSIS method analyzes the legitimacy of each CU while submission of their reports, however, it is necessary to continuously keep an eye on each activity of CUs. During the communication or data sharing/transferring process among vehicles, it is possible where intruders may further analyze the pattern and try to perform malicious activities. In order to provide a secure and transparent data sharing process, the blockchain technique is proposed that further builds a chain of each CU or device so that any single alteration in data or device can be immediately identified by the remaining nodes. Therefore, in this section, we introduce the need of blockchain while transferring/sharing the data in IoV. There are mainly three parts of consensus for ensuring secure data transferring/sharing among vehicles 1) update data block 2) TOPSIS based evaluation 3) Blockchain verification through TOPSIS. A detailed explanation of the proposed steps is given in subsequent discussion.

1) System initialization: An asymmetric cryptography is adopted for system initialization where each entity (CU) has to authenticate its identity through global TM. Further, the trust values or legitimacy of entities are analyzed through TOPSIS mechanism.
2) The participation devices may compute the trust values of each other by using TOPSIS scheme that is based upon multiple decision criteria of vehicles. Each entity analyzes the legitimacy and malicious behaviour based upon its latest trust values. The nodes having higher trust values would take part in miners for the data sharing/transferring process.
3) Consensus process: Due to a limited number of miners that are responsible for block verification and confirmation, malicious nodes may further try to launch various attacks such as DoS, false report generation etc. In order to prevent such issues, number of miners having higher trust values through TOPSIS are motivated to participate in the verification process by providing various incentives in the form of extra credits or high trust ability etc.
4) Trust value updation: After each round of consensus, vehicles download and verify their data sharing reports in vehicular Blockchain. If the previous history of data sharing is correct, the vehicle will update its trust and may further participate in forwarding the reports. Each time, the node's current trust value is updated with the previous one, if the new value is higher than previous, the block value will be updated else current value remains the same.

C. Adversary Model

The proposed CR blockchain mechanism using TOPSIS is analyzed by introducing an adversary model where intruders try to invade the communication mechanism or alter the data while sharing with various vehicles. Traditionally, to launch an adversary framework, the trusted entities are selected based upon their stake-based voting schemes. To ensure secure communication and spectrum sensing, some of the entities are distributed without the security of protection where they may be semi-trusted and vulnerable to compromise by intruders. The attackers may launch DoS, or compromise CUs for generating false reports to FC. Further, intruders may compromise miners during the data transferring/sharing process. Due to the high mobility rate, attackers may compromise only a small subset of vehicles. The possible number of threats generated by intruders are as follows:

- *False Report Generation (FRG):* It is the one where intruders compromise several CUs for generating false

reports about channel availability and submit false reports to FC.

$$FRG = \sum_{i=1}^{n} \frac{Altered\ reports}{Total\ generated\ reports} \quad (18)$$

where, n is total number of devices.

- *Compromised Miners:* Number of miners are compromised by the intruders that alter or modify the transmitted data shared among vehicles.

$$CompromisedMiners = \frac{Altered\ miners}{Total\ miners} \quad (19)$$

- *DoS attack:* It is a cyber attack in which the intruder attempts to make a device temporarily unavailable with the intent of disrupting the communication process.
- *Alteration of Transmitted Data:* The intruders aim to alter the data shared among vehicles.

The proposed mechanism is verified against various security metrics.

IV. Performance Analysis

A. System State

In this section, we first evaluate the performance of proposed TOPSIS method based on real-world data set of San-Francisco yellow cabs [45]. Recently, Kang et al. [40], have compared their proposed phenomenon with the mentioned data set. To validate the results, further, we have analyzed and compared the performance of the proposed mechanism over the baseline method against various security parameters. In the mentioned dataset, 536 taxis' mobility traces for a month are recorded. Further, less than half the number of taxis are running in urban areas within longitude and latitude of 37.81 and 37.7. There are 50 smart devices which act as CUs are deployed uniformly in the observation area of 400m $\times$ 500m size where the update period of decision criteria is 60 sec. The mobility speed of each vehicle is varying between 50 to 150 km/h depending upon the traffic congestion and weather conditions. Each vehicle is assigned with a specific weight that is computed by measuring different communicating parameters using decision-making model (TOPSIS). The IoV are categorized initially into three types according to their trust values, i.e., malicious, highly trusted, less trusted. The experiments are conducted ten times and therefore the results presented below are the average of these experiments. The major simulation parameters used during analysis are given in Table III.

B. Baseline (Existing) Method

In order to address secure data sharing/transferring through trusted miners, Kang et al. [40] have proposed a two-stage security mechanism. A reputation based scheme is used to ensure validation and verification of IoV through trusted miners. Besides, the authors have used block verification mechanism to further prevent internal threats to active miners. The proposed phenomenon is analyzed against numerical simulation through MATLAB to confirm the efficiency and security of data sharing in IoV. Our proposed mechanism is analyzed over baseline method where instead of ensuring two-stage security, the legitimate miners or peer nodes (IoV) are elected during the spectrum sensing process by the FC. The proposed mechanism uses TOPSIS method instead of a subjective logic scheme based on parameters mentioned in eq. 1, 2, 3 to elect trusted IoV and miners for data sharing and spectrum availability process. The validity of proposed mechanism is confirmed against various security metrics such as trusted values of IoV, detection rate of miners, probability of true blocks, DoS attack, false sensing report, compromised miners and alteration of transmitted data.

TABLE III: Simulation Parameters

Parameters	Setting
Coverage Range	[400, 500]m
Total number of vehicles	400
Number of taxis	536
Longitude	237.81
Latitude	37.7
Vehicles speed	[50, 150]km/h
CUs	50
Weight parameters	25, 45
Compromised vehicles rate	[10%, 90%]
Decision criteria	60 sec
Vehicles Bandwidth	20 MHz
I/O block size	[50, 500]KB

C. Results and Discussions

The effect of the proposed system for identifying the trusted IoT devices is illustrated in Figure 4. It is apparent that as the number of nodes increases in the network, the ability to measure trusted devices is analyzed efficiently. The baseline approach leads to an exponential increment and full identification of legitimate nodes after a specific number of nodes from the establishment. The reason is that during the network establishment or for a specific number of nodes (such as 20 devices in depicted Figure 4), the malicious nodes learn the pattern of legitimate devices and start behaving accordingly in the network. However, in the proposed phenomenon, the reason for the straight line is because of TOPSIS scheme where the number of devices are analyzed and traced from the start and continuously on the basis of certain communicating parameters. However, as soon as the network is polluted with

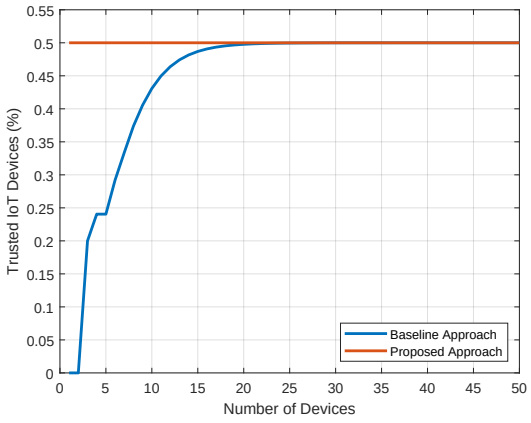

Fig. 4: Trusted IoT device

Malicious Devices/Users (MD/MU), the ability of the nodes to detect error decreases. This is due to the fact that the proposed approach identifies the legitimacy of IoT devices by computing their parameters. The devices with less service parameters are considered as MD that would not be involved during the communication process.

Figure 5 depicts the impact of the attack identification on the newly added IoT devices in the network. It can be seen that for a low attack strength, less number of IoT devices are affected and both the approaches are able to identify the alteration. However, the detection rate decrease upon the increase of compromised nodes (10% of nodes altered on each network size). However, our proposed solution enables the network to detect MD with high impact due to the fact that since the TOPSIS only allows a device to be part of the network, if it satisfies the required metrics.

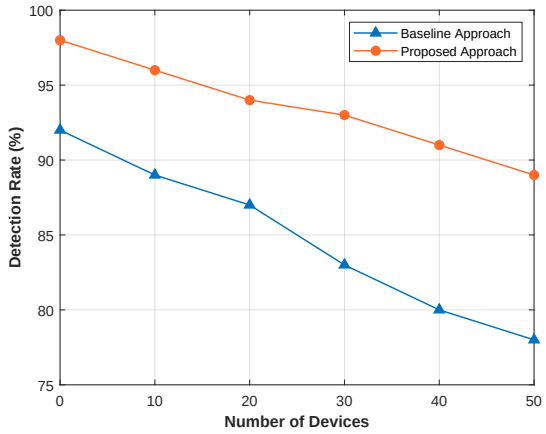

Fig. 5: Detection rate of malicious IoT

Further, the relationship among a number of reports generated by the proposed phenomenon is shown in Figure 6. The false and true reports generated by legitimate or malicious devices can be easily identified by the FC upon their immediate report submission. The TOPSIS method is attached with FC that immediately identifies the number of true or false reports generated by various secondary users or IoT devices.

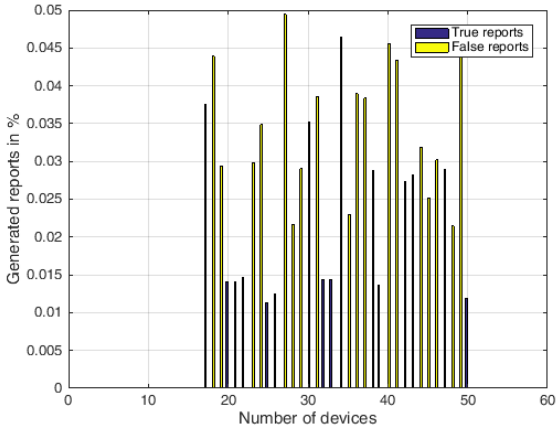

Fig. 6: Generated reports

D. Impact of Blockchain on the CRN-IoV Network

Furthermore, we have evaluated our proposal in the presence of DoS threat as depicted in Figure 7. The number of parameters with their corresponding weights successfully able to identify the malicious nodes. Further, we have created a blockchain network of initially 5 ledgers where each block contains the channel information with their respective hashes. This ledger grows further as soon as the devices generate data to be stored within the database. As depicted in Figure 7, the DoS threats can easily be measured by both the approaches through the blockchain mechanism. The proposed solution performs efficiently as compared to the baseline method because miner nodes can easily trace the malicious behavior of each device within the network.

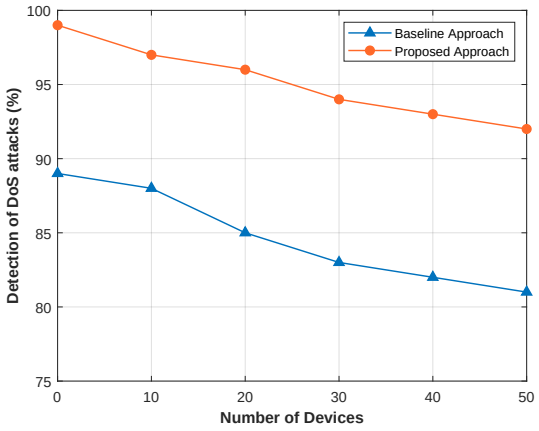

Fig. 7: DoS attack

To analyze the blockchain in CRN-IoV, I/O block size is considered as 50 and 500 kb depending upon its size. Initially, five blocks are considered where the size of the first block is 50 kb (including data and SHA256 hash), the second block is of 100 KB (consisting of data, current hash and previous block hash) and so on. The time required to create a block in the Blockchain network is 5msec.

Further, in order to check the efficiency of the proposed phenomenon, the results are analyzed against more security parameters such as message alteration and compromised miners. Here, we have equipped MDs in the network with the ability to alter and delete the recorded data as shown in Figure 8. In the proposed framework, the impact of the intrusion is limited as the devices are unable to delete or alter the data. This is due to the fact that the proposed approach is based on blockchain in the back-end which provides transparency to all the IoT devices and users so that a single change would reflect in all others' database and would become easily traceable.

Further, malicious devices may try to compromise the miner nodes during the validation and verification processes. As it can be seen from Figure 9, the number of miners compromised during this process fluctuates as a high number of devices are introduced in the network. This shows that it is very difficult to identify the authenticity of the devices at the initial levels.

The depicted Figures 8 and 9 present a zig-zag line which shows the fluctuation of the devices behavior upon increasing or decreasing the malicious nodes in the network. Further, the

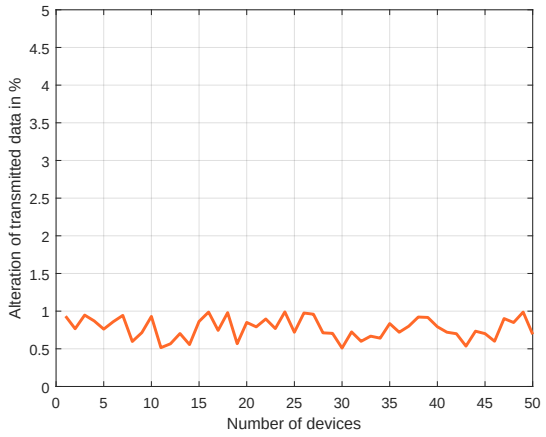

Fig. 8: Alteration of transmitted data

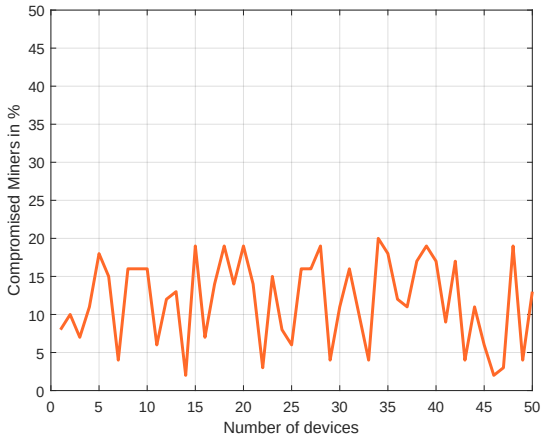

Fig. 9: Compromised miners

addition and reduction of malicious miners in the Blockchain may affect the phenomenon to analyze the behavior of each node. As soon as the nodes become older, the communication and transmission process of the number of IoT devices can be easily traced. In all the mentioned simulation results, the proposed solution is approximately 70% more efficient in terms of malicious node detection, DoS threat and computation of trusted IoT devices against the comparison of baseline approach. Further, as the number of devices is increased in the network, the proposed phenomenon may provide better results due to the parametric evaluation (based on matrix criteria evaluation as detailed in equation 7) of results with their defined weights.

V. Conclusion

In this paper, we have introduced the need for CUs in Blockchain-enabled IoV for ensuring spectrum availability and secure data transmission among vehicles. The proposed model identifies the legitimate CUs using TOPSIS method so that FC can find the correct sensing report managing the availability of channels, transfer of data over the internet and etc. Further, a blockchain is maintained within the network that keeps the chain of all vehicles or miners to ensure a secure data sharing process among each other. Further, the proposed phenomenon is significantly able to verify or validate the legitimacy of newly entered vehicles through TOPSIS mechanism. The proposed mechanism is validated extensively for different evaluation criterion's such as DoS attack, message alteration, false report generation and spectrum availability. Furthermore, simulation results suggest that our proposed model ensures approximately 70% improvement in terms of attack detection, generation of true reports against the comparison of baseline mechanism.

The further enhancement in the accuracy of spectrum sensing and data sharing by considering more parameters such as double spending attacks, authentication issues in the TOPSIS method will be reported in future communication.

References

[1] J. Worner, "Focused Delivery of Key Market Enablers in 2017/18," 2017. [Online]. Available: https://www.gsma.com/iot/newscat/mautomative-newscat/

[2] (2017) Gartner says by 2020, a quarter billion connected vehicles will enable new in-vehicle services and automated driving capabilities. [Online]. Available: http://www.gartner.com/newsroom/id/2970017.

[3] B. Ji, X. Zhang, S. Mumtaz, C. Han, C. Li, H. Wen, and D. Wang, "Survey on the internet of vehicles: Network architectures and applications," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34–41, 2020.

[4] F. Ahmad, A. Adnane, C. A. Kerrache, V. N. L. Franqueira, and F. Kurugollu, "Trust Management in Vehicular Ad-Hoc Networks and Internet-of-Vehicles: Current Trends and Future Research Directions," in *Global Advancements in Connected and Intelligent Mobility: Emerging Research and Opportunities*, F. Outay, A.-U.-H. Yasar, and E. Shakshuki, Eds. IGI Global, 2019, pp. 135–165, doi:10.4018/978-1-5225-9019-4.ch004.

[5] K. H. Law and J. P. Lynch, "Smart City: Technologies and Challenges," *IT Professional*, pp. 46–51, 2019, doi:10.1109/MITP.2019.2935405.

[6] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 119–125, 2008.

[7] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, "A Cooperative Quality-Aware Service Access System for Social Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2506–2517, 2017.

[8] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-middle Attack Resistant trust model IN connEcted vehicles," *IEEE Internet of Things Journal*, vol. 7, pp. 1–1, January 2020, (Early Access) doi: 10.1109/JIOT.2020.2967568.

[9] K. Z. Ghafoor, L. Kong, S. Zeadally, A. S. Sadiq, G. Epiphaniou, M. Hammoudeh, A. K. Bashir, and S. Mumtaz, "Millimeter-wave communication for internet of vehicles: Status, challenges and perspectives," *IEEE Internet of Things Journal*, 2020.

[10] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for Industrial Applications: Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 28–33, 2017.

[11] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi:10.1109/COMST.2015.2444095.

[12] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in Internet of Vehicles: A Review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[13] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, Sep. 2017, doi:10.1109/MCOM.2017.1600514.

[14] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in internet of things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.

[15] M. Song, C. Xin, Y. Zhao, and X. Cheng, "Dynamic Spectrum Access: From Cognitive Radio to Network Radio," *IEEE Wireless Communications*, vol. 19, no. 1, pp. 23–29, 2012.

[16] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Cooperative Spectrum Sensing in Multiple Antenna based Cognitive Radio Network using an Improved Energy Detector," *IEEE Communications Letters*, vol. 16, no. 1, pp. 64–67, 2011.

[17] C. Jiang, Y. Chen, K. R. Liu, and Y. Ren, "Renewal-Theoretical Dynamic Spectrum Access in Cognitive Radio Network with Unknown Primary Behavior," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 3, pp. 406–416, 2013.

[18] W. Xu, S. Wang, S. Yan, and J. He, "An Efficient Wideband Spectrum Sensing Algorithm for Unmanned Aerial Vehicle Communication Networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1768–1780, 2018.

[19] X. Wang, Z. Ning, X. Hu, L. Wang, B. Hu, J. Cheng, and V. C. Leung, "Optimizing Content Dissemination for Real-Time Traffic Management in Large-Scale Internet of Vehicle Systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1093–1105, 2018.

[20] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radio-based Internet of Things: Applications, Architectures, Spectrum Related Functionalities, and Future Research Directions," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 17–25, 2017.

[21] J. Eze, S. Zhang, E. Liu, and E. Eze, "Cognitive Radio-enabled Internet of Vehicles: A cooperative Spectrum Sensing and Allocation for Vehicular Communication," *IET Networks*, vol. 7, no. 4, pp. 190–199, 2018.

[22] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.

[23] G. Zyskind, O. Nathan *et al.*, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[24] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing iots in distributed blockchain: Analysis, requirements and open issues," *Future Generation Computer Systems*, vol. 100, pp. 325–343, 2019.

[25] 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, p. 3165, 2019.

[26] V. Sharma, "An Energy-Efficient Transaction Model for the Blockchain-enabled Internet of Vehicles (IoV)," *IEEE Communications Letters*, vol. 23, no. 2, pp. 246–249, 2018.

[27] M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[28] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019.

[29] L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A Secure Mechanism for Big Data Collection in Large Scale Internet of Vehicle," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 601–610, 2017.

[30] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[31] M. S. García-Cascales and M. T. Lamata, "On Rank Reversal and TOPSIS Method," *Mathematical and Computer Modelling*, vol. 56, no. 5-6, pp. 123–132, 2012.

[32] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of Blockchain in Named Data Networking-Based Internet-of-Vehicles," *IT Professional*, vol. 21, no. 4, pp. 41–47, 2019.

[33] N. Idika and B. Bhargava, "Extending Attack Graph-based Security Metrics and Aggregating their Application," *IEEE Transactions on dependable and secure computing*, vol. 9, no. 1, pp. 75–85, 2010.

[34] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem, and K. Tepe, "Technical Issues on Cognitive Radio-based Internet of Things Systems: A Survey," *IEEE Access*, vol. 7, pp. 97 887–97 908, 2019.

[35] J. Xia, Y. Xu, D. Deng, Q. Zhou, and L. Fan, "Intelligent Secure Communication for Internet of Things with Statistical Channel State Information of Attacker," *IEEE Access*, vol. 7, pp. 144 481–144 488, 2019.

[36] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A Scheme for Trustworthy Friendly Jammer Selection in Cooperative Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, 2019.

[37] Y. Qian, M. Chen, J. Chen, M. S. Hossain, and A. Alamri, "Secure Enforcement in Cognitive Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1242–1250, 2018.

[38] A. Paul, A. Daniel, A. Ahmad, and S. Rho, "Cooperative Cognitive Intelligence for Internet of Vehicles," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1249–1258, 2015.

[39] W. Hu, Y. Hu, W. Yao, and H. Li, "A Blockchain-based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles," *IEEE Access*, vol. 7, pp. 139 703–139 711, 2019.

[40] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "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.

[41] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based Cognitive Edge Framework for Sharing Economy Services in a Smart City," *IEEE Access*, vol. 7, pp. 18 611–18 621, 2019.

[42] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5g for vehicular communications," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, 2018.

[43] S. K. Datta, J. Haerri, C. Bonnet, and R. F. Da Costa, "Vehicles as Connected Resources: Opportunities and Challenges for the Future," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 26–35, 2017.

[44] Y.-J. Lai, T.-Y. Liu, and C.-L. Hwang, "Topsis for MODM," *European Journal of Operational Research*, vol. 76, no. 3, pp. 486–500, 1994.

[45] M. A. Hoque, X. Hong, and B. Dixon, "Analysis of Mobility Patterns for Urban Taxi Cabs," in *2012 international conference on computing, networking and communications (ICNC)*. IEEE, 2012, pp. 756–760.