NSS
Neutrosophic Sets and Systems, Vol. 60, 2023
University of New Mexico

Decarbonization Transportation: Evaluating Role of Cyber Security in Transportation sector based on Neutrosophic Techniques in a Climate of Uncertainty

Nissreen El Saber[1], Mona Mohamed[2], and Nabil M. AbdelAziz[1]
[1]Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt.
Emails: naelsaber@fci.zu.edu.eg; nmabedelaziz@fci.zu.edu.eg
[2]Higher Technological Institute, 10th of Ramadan City 44629, Egypt; mona.fouad@hti.edu.eg

Abstract

Recently, transport systems that produce low levels of carbon emissions have emerged as an essential component of several nations' goals for achieving sustainable development. These systems also play a very significant role in the process of developing low-carbon cities. On the other hand, the safety of low-carbon modes of transport has been put in jeopardy in several different ways. For instance, assaults that result in a denial of service present a significant danger to the networks that connect electric cars to the grid. Several different strategies for defending against these dangers have been developed to lessen their impact. However, these strategies are only applicable to certain kinds of situations or assaults. Therefore, the purpose of this paper is to examine the security element from a holistic approach, present an overview of the obstacles and future directions of cyber security technologies in low-carbon transportation, and overcome such challenges. To begin, the low-carbon transport services are positioned in this article based on the idea of low-carbon transport and the significance of low-carbon transport. After that, using the network's design and the manner of communication as a lens, this article defines the common threats posed by attacks on the network. An additional consideration is given to the associated defensive technologies as well as the pertinent security recommendations, this time from the point of view of data security, network management security, and network application security. To improve this notion of safeguarding the gride and communication, it is necessary to evaluate ability of network against sniffing and spoofing or from any various methods of attacks. This motivates the study to employ Multi- Criteria Decision Making (MCDM) entailed in entropy for weighting the benchmarks which employed in Combined Compromise Solution (CoCoSo) toward obtaining optimal intelligent transportation systems (ITrSs) through ranking various ITrSs. In this study the utilized techniques are powered by uncertainty theory is Triangular Neutrosophic Sets (TriNSs). These utilized techniques contributed to constructing robust hybridization model. This model implemented in real case study to ensure its validity on decision making.

Keywords: Low-Carbon Transportation; Sustainable Environment; Cyber security; Holistic Approach; Multi- Criteria Decision Making (MCDM); Triangular Neutrosophic Sets (TriNSs).

1. Introduction

Both the energy and transport industries are responsible for the majority of the world's total carbon emissions. The transformation of energy and transport networks into low-carbon models is unavoidable if the strategic aim of reaching "carbon peaking and neutralization" is to be accomplished [1].

Our everyday lives, including the industries of energy and transportation, are being revolutionized by the spread of digital technology. Digitalization is a significant development that gives choices for reducing energy demand and carbon emissions [2]; nevertheless, it has been questioned as to whether the local energy savings from networked digital devices might compensate for the increased energy usage of the devices. Digitalization is an important trend that provides alternatives for reducing energy

demand and carbon emissions. Additionally, digital technologies have the potential to contribute to the intelligent and environmentally friendly design of the future generation of transportation systems.

Both the academic world and the business world are interested in how decarbonization might be facilitated in a timely and cost-effective manner by digitalization [3]. This is an important development. Digitization comprises sensing, transmission, and computing, i.e., data production, data transfer, data storage and transformation, and data application (data value generation). When seen through the lens of the data value stream, the production of data of a high standard is strongly dependent on the development of infrastructure, which may include sensors for energy and transportation. In the meanwhile, the development of technologies known as 5G and 6G helps to speed up the transmission of data, which is necessary to meet the requirements of the big data age for the timely delivery of large quantities of data. Data has the potential to generate values in a wide variety of application situations, and digitalization may be able to contribute to the industry's overall growth and success if it is supported by more complex procedures and algorithms.

The dependability and stability of low-carbon transportation systems are significantly improved when cyber security measures are included [4]. To begin, ensuring the confidentiality, enforceability, and non-repudiation of one's data is the primary responsibility of a company's data security team [5]. Second, the implementation of network management security, which should include trust management, misbehavior detection, an intrusion detection system, and a firewall, is required in order to guarantee the dependability of the data that is sent inside a network system, as well as its integrity and accuracy. In conclusion, personalized network applications result in new security needs, and it is important to pay attention to both edge computing security and software-defined security in this context.

In order to accomplish this goal, the focus of this article is on the analysis and research of the functioning of a low-carbon ecosystem, with the primary emphasis being placed on the cyber security of low-carbon transportation. The purpose of this piece is to shed light on the significance and effect of cyber security in low-carbon transportation, as well as to encourage the coordinated development of electric cars, transportation, energy, information, and cyber security. Specifically, the article will focus on revealing the relevance and impact of cyber security in low-carbon transportation. The following is the most important contributions that this article makes:

- The low-carbon transport service is positioned in this assessment based on the idea of low-carbon transport and the significance of low-carbon transport.
- A discussion of the problems with cyber security and the solutions to those problems.
- Challenges and potential avenues of study have been highlighted in light of the recent trend toward the development of low-carbon modes of transportation.
- Construct evaluation model responsible for evaluating intelligent transportation systems.
- Applying the constructed evaluation model in real enterprises of transportation.

2. Theoretical Background

The development of low-carbon transportation might be helped forward by the integration of transportation, energy, and information networks. On the other hand, several application scenarios and information interactions in low-carbon transportation would expose its vulnerabilities to attack. A security defense system must be implemented in order to repel assaults in application situations or communication modalities. In the first part of this section, we will go through several common application situations and low-carbon transportation component types. In the second place, it examines common information and communication technologies, such as E-Mobility, smart grids, in-vehicle connectivity, and communication between vehicles and other things. The latter part of this section focuses on the possible cyber dangers and common assaults on low-carbon transportation.

2.1 Carbon-neutral transportation

Charging stations and battery swapping stations are potential sources of electricity for electric cars [6]. Charging stations, battery swap stations, and other similar facilities may all get their power from

the smart grid. The demand for energy from electric cars is processed through charging stations and battery swap stations, which function as an intermediate.

The commercialization of electric cars is making steady progress due to the many positive impacts these vehicles may have on their surrounding environments. Traditional automobile manufacturers, such as Mercedes-Benz and BMW, as well as the electric vehicle manufacturer Tesla, have been preparing their transition towards the electrification of vehicles in response to the current worldwide trend.

Compatibility is one of the fundamental ideas behind the smart grid, which encompasses both centralized and decentralized power-producing infrastructures as well as access to a wide variety of energy storage solutions. The term "distributed power" refers to the production and storage of electricity by a wide variety of low-capacity devices that are linked to either the smart grid or the distribution system. These distributed energy resources are also known as "distributed energy resources." The distributed energy resources system is a decentralized, modular, and more adaptable technology that utilizes renewable energy such as solar energy and wind energy on a local scale. The system also makes use of modular solar panels and wind turbines. If not, centralized electricity would be provided by conventional power stations, which include coal, gas, and nuclear power plants, as well as hydropower dams and large-scale solar power stations. The smart grid that is enabled by 5G and artificial intelligence will contribute to an improvement in the efficiency of energy transit and utilization.

The low battery capacity of electric cars combined with the length of journeys taken inside metropolitan areas results in the need for regular charging of electric vehicles. Charging stations are often installed in areas that have a large concentration of electric vehicles, such as shopping malls and parking lots. In general, this means that charging stations are located in high-density areas. In the event that the charging station is unable to detect the arrival of electric cars that have a need for charging, however, there is a possibility that a charging service congestion may arise. Because of advances in communication technology between vehicles and other objects, it is now feasible to exchange information of this kind in order to supervise the charging process in the most effective manner.

2.2 Information and communication technologies applied to low-carbon modes of transportation

In spite of the fact that significant attention has been dedicated to the development of electric cars from both academic and industrial perspectives, the growth of the electric vehicle sector is being hampered by problems such as insufficient charging facilities, a lack of standardization, and inconsistent norms. Electric cars and charging stations are seeing tremendous expansion as a direct result of the concerted efforts of companies and governments all over the globe.

The charging pile's communication method may primarily be broken down into two categories: wired communication and wireless communication modalities. The most common forms of the wired communication method include industrial serial bus and wired Ethernet, among others. When it comes to data transfer, industrial serial bus systems are more dependable; nevertheless, they come with a number of drawbacks, including high complexity, low communication capacity, poor flexibility, high building costs, and limited scalability. Despite its complicated wiring, limited flexibility, high construction cost, and limited expansibility, the wired Ethernet network has a larger capacity and provides data transfer that is dependable.

2.3 Disputes over safety in low-carbon modes of transportation

In the recent past, the idea of a smart grid has emerged as a result of advancements in information and communications technologies. The beneficial information is constantly being transmitted and monitored inside the smart grid in order to initiate decision-making on the management of the power system. However, despite the fact that the access network makes the operation of the system more efficient, this improvement will put the system's security at risk since it is dependent on the flow of

information. Because communication networks are susceptible to cyber assaults and hostile infiltration, the smart grid is not immune to the attacks that hackers have been carrying out in increasing numbers over the last several years, regardless of whether they are motivated by profit or politics.

"GPS spoofing" is a method that may be used to attack an autonomous vehicle's multi-sensor fusion positioning technique, which ultimately results in the car losing control of itself. This was discovered via research. This safety concern has sounded the alarm for manufacturers, who in recent years have increased their efforts to commercialize autonomous driving.

2.4 Attacks that are typical in low-carbon transportation

One of the most significant difficulties that nations all over the globe are now confronting is that of maintaining adequate levels of cyber security. The advancement and promotion of low-carbon modes of transport are impossible to do without the accompaniment of cyber security [7]. The foundation of successful low-carbon city development is a foolproof and comprehensive cyber security protection and prevention system. Nevertheless, low-carbon transport is being subjected to a large number of assaults and safety hazards. Jamming, spoofing, data dimension, denial of service, botnet, and sybil assaults are the most common types of low-carbon transportation threats [8]. Other types of attacks include dos attacks and data dimension attacks. Be aware that, in addition to traditional forms of cyber assault, there is also the possibility of a physical attack, which involves the use of forceful methods to target electric cars, charging piles, and other forms of firmware, among other things. In this context, it is necessary to perform routine safeguarding and maintenance on such important facilities.

3. Safety Measures for Network Management

The dependability, integrity, and accuracy of data that is shared inside a network system are ensured by the security of network management, which includes trust management, identification of inappropriate behavior, intrusion detection systems, and firewalls.

3.1 Confidence administration

Standard technologies that need much greater processing power, such as intrusion detection, password encryption, and decryption technology, are not suitable because of the restricted capacity of cars. Alternately, the function of the trust mechanism is to assess the amount of confidence that may be placed in vehicles by using the interaction history of those vehicles. By using this as assessment advice, it is possible to give up on hostile cars and promote trustworthy vehicles for data exchange.

The majority of the literature that is based on the entity-based trust model assesses the trustworthiness of vehicles. In this instance, direct trust and indirect suggestion trust are used together in order to identify automobiles that are not to be trusted or that are harmful.

Model of trust that is based on data, the model of trust that is based on data seeks to determine how reliable the data level is. In this case, the trust model calls for the collection of data from a wide range of sources, such as the cars themselves, their immediate neighbors, and roadside units.

The mixed trust model is one that, by default, incorporates the positive aspects of both traditional and alternative models of trust. Not only does it determine the degree to which cars can be trusted, but it also computes the accuracy of the data. The trustworthiness of vehicles has an effect on the dependability of data as a result of the influence of contact behavior, and the trustworthiness of data, in turn, reflects the dependability of vehicles as a result of the forwarding route that a data will be traveled. This is the purpose of the combined trust model, and it is inherent in its design.

3.2 Detection of inappropriate behavior

It is also possible to identify malicious vehicles based on the actions taken by network participants. These actions include forwarding, altering, discarding, and selective discarding of data. The benefit of using techniques that are based on network behavior is that they are wholly unaffected by the information that is being sent.

It is challenging to assess the fabricated data when there are just a few cars collecting enough messages for detection. Another way of saying this is that it is challenging to determine the forged data based only on the data content level.

3.3 Intrusion detection system

Because of power outages and natural calamities, the smart grid is very susceptible to denial of service assaults. Denial-of-service attacks are made with the intention of delaying, blocking, or otherwise disrupting communications, which may have a significant negative impact on the functioning of a network. An intrusion detection system that is based on deep learning has the potential to improve the detection and mitigation of denial-of-service attacks [9]. For the purpose of analyzing the features of information flow, it is put at the smart grid's edge. The typical pattern of behavior shown by information flow is created on the basis of spatiotemporal characteristics and context relations. In addition to that, the real-time schedulability analysis will extract the timing requirements as well as the model parameters of the information flow. After that, the intrusion detection system will develop a real-time model that precisely characterizes the temporal characteristics. This model will then be used to reflect the typical behavior of smart grid systems. Finally, with the help of packet attribute analysis and a data consistency model that is based on deep learning, it is possible to determine the usual behavior pattern of a physical information system as well as the origin of a cyber-assault.

Because of its usefulness in rapidly detecting assaults, the intrusion detection system garners a lot of attention. The network or host intrusion detection system will, as a general rule, identify any irregularity in the system and sound an alert if it exists. The intrusion detection system may be broken down into two groups according to the technological basis of intrusion detection:

- Signature-based intrusion detection system: This intrusion detection system analyzes known attacks to extract their distinguishing features and patterns, which is called the signature [10]. The signature-based intrusion detection system has the advantage of a high detection rate for known attacks, but the disadvantage is that it is not able to detect unknown or new attacks.
- Using supervised or unsupervised learning approaches to construct models based on characteristics, anomaly-based intrusion detection systems are another form of intrusion detection systems that are also known as behavior-based intrusion detection systems [11]. The model is able to distinguish between regular and aberrant patterns of network traffic, and it also has the power to detect undiscovered and novel forms of assault. Statistical and machine learning methods are used in the execution of this approach.

3.4 Firewall

The divide between public and private networks may be represented by a firewall. It is able to identify assaults and filter the flow of harmful traffic via the network [12]. The next-generation firewall has the capability to integrate denial-of-service attack detection technologies with network protocol identification capabilities. The former is used to filter attack flow and lower the danger of attack, while the latter is used to deal with injection and spoofing. Both of these functions are important for preventing attacks.

It is possible to identify the internet protocol address of the host computer or server that is connected to the network thanks to the smart grid system. Therefore, the function of the firewall known as packet filtering may be accomplished using a whitelist. To begin, the firewall analyses the flow of network traffic based on the kind of protocol, the number of ports, and the internet protocol address of the destination. This allows it to determine whether or not the traffic conforms to the standards, restrictions, and whitelists that have been set. After that, the position of the firewall may be adjusted so that it is in accordance with the structure of the smart grid network.

In order to defend against a wide range of assaults, firewalls for electric vehicles are also now in development. The network configuration information for an in-vehicle network is generally unchangeable, which is one of the properties of this kind of network. In most cases, the original

equipment manufacturer is in possession of a communication matrix or database that lays out the guidelines for how electronics inside the vehicle are to communicate with one another. As a direct consequence of this, the "whitelist" filtering rules are often used as the foundation for the firewall technology used in an in-vehicle network.

4. Motivations of Study

Two significant trends in the upcoming decades are expected to be decarbonization and digitalization [13]. Massive amounts of data will be generated as the already pervasive process of digitization proceeds, particularly in the energy and transportation networks. How this data may support and promote data security has become a critical concern.

Hence. This study focuses on embracing cybersecurity technologies in intelligent transportation to guarantee confidentiality, unforgeability, and non-repudiation for smart grid. Accordingly, it is important to evaluate the enterprises of transportation which are deploying and embracing cybersecurity toward digitalization and decarbonization dimensions. We are conducting a survey for transportation enterprises for contributing to the evaluation process.

Accordingly, we constructed an evaluation model which is responsible for evaluating the enterprises which obtained from the conducted survey. This model relies on mathematical techniques and uncertainty theory to improve decisions in uncertainty environments [18-22].

5. Methodology of Evaluation

5.1 Recognition of principal ingredients

- One of the important procedures in study's evaluation methodology is recognizing principal and influential aspects.
- These aspects entailed in set of benchmarks {Bs}= {b_1, b_2,b_3,…b_n} also, set of nominees of Transportation enterprises systems as {TESs}={TES_1,TES_2,…TES_n}.
- Choice and communicate with decision makers (DecMs) who related to our interested study's scope.

5.2 Express the most and least significant benchmark through benchmarks' weights

- We are leveraging TriNSs scale in [14],[15] to contribute to evaluation process where DecMs are rating criteria based on the determined scale.
- Entropy is employed as a technique of MCDM techniques with the support of TriNSs s as branch of neutrosophic theory for generating criteria's weights. Hence, Neutrosophic decision matrices are constructed based on DecMs'preferences.
- Score function in Eq. (1) turns the constructed matrices to deneutrosophic matrices as mentioned in Ref [16].

$$s(b_{ij}) = \frac{(C_{ij}+D_{ij}+F_{ij})}{9} * (2 + \alpha - \beta - \theta) \quad (1)$$

where C_{ij}, D_{ij}, F_{ij} pointed to lower, middle, upper. Also, α, β, θ are truth, indeterminacy, and falsity.

- Eq.(2) aggregates deneutrosophic matrices into single decision matrix to construct an aggregated matrix.

$$Z_{ij} = \frac{(\sum_{j=1}^{N} b_{ij})}{S} \quad (2)$$

Where b_{ij} refers to value of criterion in matrix, S refers to number of decision makers.

- An aggregated matrix is normalizing through Eq. (3).

$$\mho_{ij} = \frac{z_{ij}}{\sum_{j=1}^{m} z_{ij}} \quad (3)$$

Where $\sum_{j=1}^{m} z_{ij}$ represents sum of each criterion in aggregated single decision matrix per column

- Entropy computes easily via utilizing Eq. (4).

$$e_{j=-h\sum_{i=1}^{m}\upsilon_{ij}}\ \ln \mho_{ij} \tag{4}$$

$$\text{Where} h = \frac{1}{\ln(Q)} \tag{5}$$

Q refers to number of alternatives

- Weight vectors generated through leveraging Eq.(6).

$$w\_vector_{j=\frac{1-e_j}{\sum_{j=1}^{n}(1-e_j)}} \tag{6}$$

5.3 Find out the best and the worst intelligence transportation system accordance to cyber security through ranking

Herein we are exploiting CoCoSo according to [17] as MCDM ranker technique for ranking nominees of ITrSs through improving the utilized ranker technique by TriNSs through implementing several steps:

- an aggregated decision matrix generated from previous steps of obtaining benchmarks' weights has been leveraged. Furthermore, Eq.s (7) and (8) are responsible for normalizing single matrix.

$$Nor_{ij} = \frac{Z_{ij-\min(Z_{ij})}}{\max(Z_{ij})-\min(Z_{ij})}\ \text{, for beneficial criteria} \tag{7}$$

$$Nor_{ij} = \frac{\max(Z_{ij})-Z_{ij}}{\max(Z_{ij})-\min(Z_{ij})}\ \text{, for non-beneficial criteria} \tag{8}$$

- Sum of weighted matrix is generated based on Eq. (9).

$$Sum\_weighted_i = \sum_{j=1}^{n} w\_vector_j * Nor_{ij} \tag{9}$$

- Eq. (10) is deploying for calculating power of weighted matrix.

$$Power_j = \sum_{j=1}^{n}\left(Nor_{ij}\right)^{Sum\_weighted_{ij}} \tag{10}$$

- Three different appraisal score for ITrSs candidates are calculating through following Eq.s.

$$Score_{ia} == \frac{S_i+P_i}{\sum_{i=1}^{m} S_i+P_i} \tag{11}$$

$$Score_{ib} = \frac{S_i}{\min_i S_i} + \frac{P_i}{\min_i P_i} \tag{12}$$

$$Score_{ic} = \frac{\lambda S_i+(1-\lambda)P_i}{\lambda \max_i S_i+(1-\lambda)\max_i P_i}\ , 0 \le \lambda \le 1 \tag{13}$$

Where S_i indicates to sum of each raw in sum of raw in weighted matrix whilst P_i refers to sum of raw in power of weighted matrix.

- The final rank is obtaining via Eq. (14).

$$K_{i=}(K_{ia} * K_{ib} * K_{ic})^{1/3} + \frac{1}{3}(K_{ia} + K_{ib} + K_{ic}) \tag{14}$$

6. Numerical case study

The validation process is considered important in this study. Hence, we applied our constructed model of evaluation on real transportation enterprises which embracing study's notion. The evaluation for systems of these enterprises is performed based on set of benchmarks.

The validation process is conducting through following dimensions:

6.1 First dimension: benchmarks and intelligent transportation systems(alternatives).

- The ITrSs which embracing study's notion are identifying where four alternatives are contributed to validation process. Accordingly, the benchmarks are determined as in Figure 1.
- Therefore, five DecMs are contributed to rate alternatives of ITrSs based determined benchmarks through utilizing triangular Neutrosophic scale in [15].

6.2 Second dimension: Determining benchmark's weights.

- An aggregated matrix is constructed through calculating average for five Neutrosophic decision matrices as listed in Table 1.
- Whilst Table 2 represents normalization of an aggregated matrix.
- Entropy matrix is constructed based on Eqs. (4),(5) and Table 3 is generated.
- Moreover, vector of weights is generated through implementing Eq.(6) and Figure 2 represents benchmarks' criteria. According to this Figure B3 considered the optimal criterion where its value of weight is the highest compared with others otherwise B4 where its value of weights is the least one.

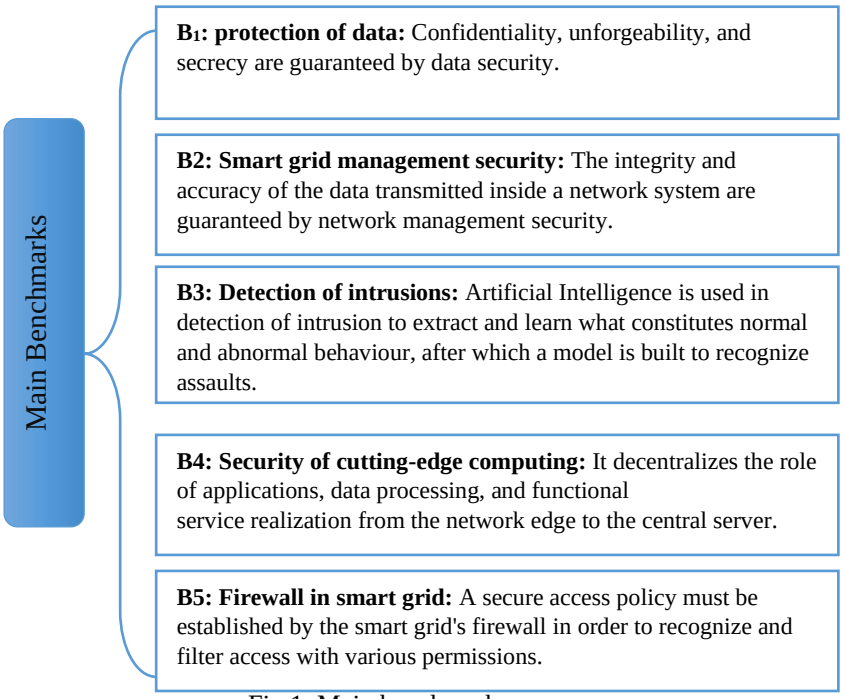

Fig.1. Main benchmarks

Table1. An aggregated decision matrix

	B_1	B_2	B_3	B_4	B_5
$ITrSs_1$	4.656666667	4.946666667	5.456666667	4.283333333	5.253333333
$ITrSs_2$	5.583333333	6.103333333	4.726666667	5.593333333	6.706666667
$ITrSs_3$	4.683333333	4.653333333	6.123333333	4.64	4.81
$ITrSs_4$	6.65	4.596666667	7.233333333	5.623333333	5.996666667

Table2. Normalized an aggregated decision matrix.

	B_1	B_2	B_3	B_4	B_5

ITrSs$_1$	0.215852905	0.2436782	0.23180402	0.212677921	0.230746706
ITrSs$_2$	0.258807169	0.3006568	0.20079298	0.277722608	0.294582723
ITrSs$_3$	0.217088999	0.2292282	0.26012461	0.230387289	0.211273792
ITrSs$_4$	0.308250927	0.2264368	0.30727839	0.279212181	0.263396779

Table3. Entropy Matrix

	B$_1$	**B$_2$**	**B$_3$**	**B$_4$**	**B$_5$**
ITrSs$_1$	-0.330936629	-0.344050886	-0.338865722	-0.329220395	-0.338374972
ITrSs$_2$	-0.349822408	-0.361325095	-0.322369282	-0.355799453	-0.360037656
ITrSs$_3$	-0.33159213	-0.337661701	-0.350282368	-0.338207048	-0.32844632
ITrSs$_4$	-0.362762369	-0.33632417	-0.362588849	-0.356214232	-0.351395988
$-\mathrm{h}\sum_{i=1}^{m} \mho_{ij}\ ln\mho_{ij}$	-1.375113537	-1.379361852	-1.374106221	-1.379441128	-1.378254936

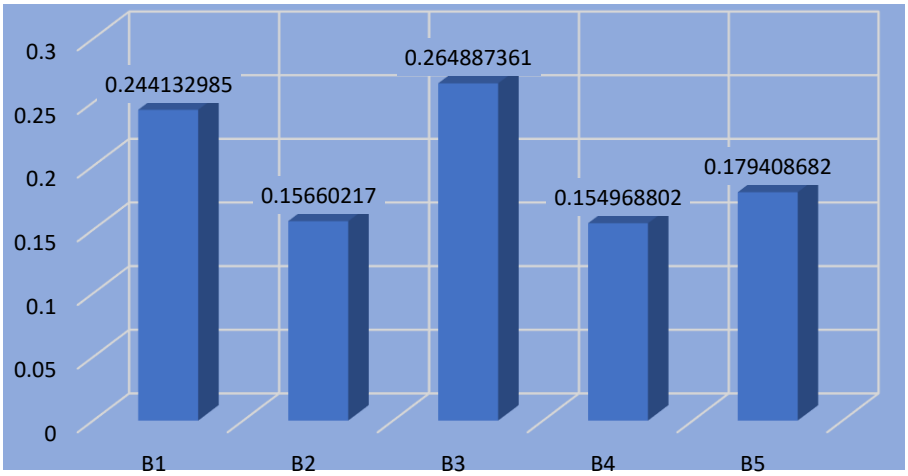

Fig.2. benchmarks Weights

6.3 Third dimension: Ranking alternatives of ITrSs

- In this dimension, an aggregated matrix which generated from second dimension is normalized by Eq.(7) where benchmarks are considering beneficial and Table 4 has been generated.
- Weighted decision matrix has been produced through multiplying normalized matrix with weights of benchmarks which generated from entropy-TriNSs. The result of this process is illustrated in Table 5.
- The power of sum weighted matrix has been computed via Eq.(10) and results are showcased in Table 6.
- Candidates' appraisal scores have been calculated through Eq.(11),(12),(13). And its scores are appeard in Table 7. According to this Table, we concluded that ITrS4 is the best otherwise ITrS1 is the least one.
- Finally, the final rank for candidates ITrSs. Eq.(14) is utilized for obtaining the candidates' final rank which showcased in Figure 3 where the results in this Figure agreed with ranking in Table7and emphasized that ITrS4 is the best otherwise ITrS1 is the least one

Table 4. Normalized an aggregated matrix based on CoCoSo-TriNSs

	B_1	B_2	B_3	B_4	B_5
$ITrS_1$	0	0.232300885	0.291223404	0	0.233743409
$ITrS_2$	0.464882943	1	0	0.97761194	1
$ITrS_3$	0.013377926	0.037610619	0.557180851	0.266169154	0
$ITrS_4$	1	0	1	1	0.625659051

Table 5. Weighted decision matrix based on CoCoSo-TriNSs

	B_1	B_2	B_3	B_4	B_5
$ITrS_1$	0	0.036378823	0.077141399	0	0.041935597
$ITrS_2$	0.113493261	0.15660217	0	0.151499351	0.179408682
$ITrS_3$	0.003265993	0.005889905	0.147590165	0.041247915	0
$ITrS_4$	0.244132985	0	0.264887361	0.154968802	0.112248666

Table 6. Powe of Weighted decision matrix based on CoCoSo-TriNSs

	B_1	B_2	B_3	B_4	B_5
$ITrS_1$	0	0.795650225	0.721240842	0	0.770453377
$ITrS_2$	0.829445018	1	0	0.996497271	1
$ITrS_3$	0.348810625	0.598260777	0.856480736	0.814549312	0
$ITrS_4$	1	0	1	1	0.919308384

Table 7. Various scores of candidates

	K_{ia}	K_{ib}	K_{ic}	Rank
$ITrS_1$	0.169858453	1.672656822	1.605882339	4
$ITrS_2$	0.307824659	1.14460306	2.910247763	2
$ITrS_3$	0.195815279	1.713475377	1.851284357	3
$ITrS_4$	0.326501609	1.672656822	3.086824095	1

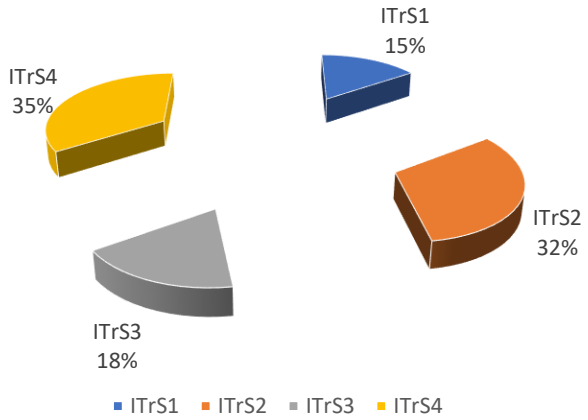

Fig.3. Final Score for various ITrSs candidates

7. Future directions

In point of fact, there are still questions that need answers from communities. The fundamental objective is to advance the intelligence level of cars within a low-carbon transportation system in order

to make use of more potent digitalized services and cyber security technologies. This will be accomplished via the promotion of this direction. In accordance with the integrated control for low-carbon transportation, it is desirable to investigate other new approaches such as detachable security technology and zero-knowledge proof. These hypothetical trajectories are presented in the following order:

- The information and communication systems of automobiles, artificial intelligence, software, the Internet, and other technologies are deeply incorporated into the intelligent linked vehicles.
- Combining several technologies in order to perform certain tasks has become more common in recent years, thanks both to the ongoing development of existing technologies and the birth of brand-new technologies in fields ranging from hardware design to software algorithms. However, these technologies are not coupled to a particular degree, and they also need a balance to be struck between their functions and their performances.
- People will have a greater propensity to purchase electric cars when the policies that promote them and when environmental preservation are taken into consideration. The proliferation of electric cars has brought to light the pressing need to improve internet connectivity inside vehicles and their ability to communicate with one another. Then, when a significant number of electric cars are linked to the smart grid, the influence on the system of the smart grid will become more significant. In light of this, one of the potential areas of focus for future study is the integrated control issue of smart charging for electric vehicles and collaborative technology for smart grids.
- Large amounts of disparate data coming from a variety of sources are required to ensure the safety of intelligent transportation systems. Zero-knowledge proof is progressively being included in intelligent transportation systems in order to guarantee the system's computational security. The goal of zero-knowledge proof is to convince the verifier that the prover is in possession of the proof without revealing any confidential information.
- In light of the fact that low-carbon transport is still in its infancy, it is still required to devise high-level policy and speed up technological innovation.

8. Conclusion

Most recent studies emphasized that energy and transportation systems are becoming more intelligent, sustainable, and efficient courtesy to digital technologies like sensors, 5G, IoT, and data trading.

Hence, this article begins by providing an introduction to the idea of low-carbon transport as well as its historical context. This is done in light of the growing focus on attaining low-carbon transport and the requirement of securing the system via the use of Cybersecurity technology ٥n the era of intelligent transportation. After that, this article classifies and reviews emerging defense technologies from the aspects of data security, network management security, and network application security, covering up-to-date technical advances that have been contributing to communities. The classification and review process based on identifying typical attacks within the ecosystem of a low-carbon transportation system, and it covers recent technical advancements that have been helping communities. Also, evaluating the transportation enterprises which embracing our notion of deploying technologies that support cybersecurity toward safeguarding smart grid and information against any attack. Through the survey that was conducted for the enterprises, we communicated with four ITrSs which contribute to the evaluation process.

Hence, we constructed robust hybrid model which relied on mathematical techniques of MCDM techniques. These techniques are hybridized with uncertainty theory of neutrosophic which has main role of supporting MCDM techniques in situations characterized with ambiguity and inability to preferences and making decisions. Moreover, we employed entropy based on TriNSs to obtain weights for five benchmarks. The obtained benchmarks' weights are contributed to the process of ranking four ITrSs through multiplying the weights by normalized matrix. This matrix generated from utilizing CoCoSo based on TriNSs which responsible for ranking ITrSs after that recommending the best and worst ITrS.

In addition to the existing contribution, this article highlighted several future directions that cover the cyber-secure low-carbon transportation system from the evolution of vehicles, compatibility of defense technologies integration, and potential impact on unlocking the cyber security and system reliability. These future directions cover all these topics and more.

Funding: "This research received no external funding."

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] J. Song, G. He, J. Wang, and P. Zhang, "Shaping future low-carbon energy and transportation systems: Digital technologies and applications," *iEnergy*, vol. 1, no. 3, pp. 285–305, 2022, doi: 10.23919/IEN.2022.0040.

[2] Maxbuba Ismailova,Nargiza Alimukhamedova, Potential Pitfalls of Data Fusion Digitalization in Microfinance Context, Fusion: Practice and Applications, Vol. 12 , No. 2 , (2023) : 98-108 (Doi : https://doi.org/10.54216/FPA.120208)

[3] O. Lah, "Decarbonizing the transportation sector: policy options, synergies, and institutions to deliver on a low-carbon stabilization pathway," *WIREs Energy Environ.*, vol. 6, no. 6, p. e257, Nov. 2017, doi: https://doi.org/10.1002/wene.257.

[4] Lobna Osman, Olutosin Taiwo, Ahmed Elashry, Absalom E. Ezugwu, Intelligent Edge Computing for IoT: Enhancing Security and Privacy, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 55-65 (Doi : https://doi.org/10.54216/JISIoT.080105)

[5] Mehmet Merkepci,Mohammad Abobala, Security Model for Encrypting Uncertain Rational Data Units Based on Refined Neutrosophic Integers Fusion and El Gamal Algorithm, Fusion: Practice and Applications, Vol. 10 , No. 2 , (2023) : 35-41 (Doi : https://doi.org/10.54216/FPA.100203)

[6] D. Qiao *et al.*, "Toward safe carbon–neutral transportation: Battery internal short circuit diagnosis based on cloud data for electric vehicles," *Appl. Energy*, vol. 317, p. 119168, 2022, doi: https://doi.org/10.1016/j.apenergy.2022.119168.

[7] Raaid Alubady, Rawan A.shlaka, Hussein Alaa Diame, Sarah Ali Abdulkareem, Ragheed Hussam, Sahar Yassine, Venkatesan Rajinikanth, Blockchain-based e-Medical Record and Data Security Service Management based on IoMT resource, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 2 , (2023) : 86-100 (Doi : https://doi.org/10.54216/JISIoT.080207)

[8] L. Guo, B. Yang, J. Ye, J. M. Velni, and W. Song, "Attack-Resilient Lateral Stability Control for Four-Wheel-Driven EVs Considering Changed Driver Behavior Under Cyber Threats," *IEEE Trans. Transp. Electrif.*, vol. 8, no. 1, pp. 1362–1375, 2022, doi: 10.1109/TTE.2021.3102134.

[9] Ehab R. Mohamed,Heba M. Mansour,Osama M. El-Komy, An efficient fusion method for Protecting Software-Defined Networks Against ARP Attacks: Analysis and Experimental Validation, Fusion: Practice and Applications, Vol. 12 , No. 1 , (2023) : 08-23 (Doi : https://doi.org/10.54216/FPA.120101)

[10] J. Díaz-Verdejo, J. Muñoz-Calle, A. Estepa Alonso, R. Estepa Alonso, and G. Madinabeitia, "On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks," *Applied Sciences* , vol. 12, no. 2. 2022. doi: 10.3390/app12020852.

[11] Ashish Dixit, R. P. Aggarwal, B. K. Sharma, Aditi Sharma, Safeguarding Digital Essence: A Sub-band DCT Neural Watermarking Paradigm Leveraging GRNN and CNN for Unyielding Image Protection and Identification, Journal of Intelligent Systems and Internet of Things, Vol. 10 , No. 1 , (2023) : 33-47 (Doi : https://doi.org/10.54216/JISIoT.100103) '

[12] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, and J. Yusupov, "Automated Firewall Configuration in Virtual Networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 2, pp. 1559–1576, 2023, doi: 10.1109/TDSC.2022.3160293.

[13] E. Hittinger and P. Jaramillo, "Internet of Things: Energy boon or bane?," *Science (80-.).*, vol. 364, no. 6438, pp. 326–328, 2019.

[14] A. Gamal and M. Mohamed, "A hybrid MCDM approach for industrial robots selection for the automotive industry," *Neutrosophic Syst. with Appl.*, vol. 4, pp. 1–11, 2023.

[15] I. Elhenawy, "Intelligent Healthcare : Evaluation Potential Implications of Metaverse in Healthcare Based

on Mathematical Decision- Making Framework," vol. 12, 2023.

[16] K. A. Eldrandaly, N. El Saber, M. Mohamed, and M. Abdel-Basset, "Sustainable Manufacturing Evaluation Based on Enterprise Industry 4.0 Technologies," *Sustainability*, vol. 14, no. 12, p. 7376, 2022.

[17] S. F. Al-baker and M. Mohamed, "Exploring the Influences of Metaverse on Education Based on the Neutrosophic Appraiser Model," vol. 23, no. 01, pp. 134–145, 2024.

[18] Ahmed Abdelaziz,Alia Nabil Mahmoud, COVID-19 vaccine choice using the multi-criteria decision making method under uncertainty, American Journal of Business and Operations Research, Vol. 8 , No. 1 , (2022) : 40-46 (Doi : https://doi.org/10.54216/AJBOR.080104)

[19] Shilpi Pal,Avishek Chakraborty, Triangular Neutrosophic-based EOQ model for non-Instantaneous Deteriorating Item under Shortages, American Journal of Business and Operations Research, Vol. 1 , No. 1 , (2020) : 28-35 (Doi : https://doi.org/10.54216/AJBOR.010103)

[20] A. Abdel-Monem, N. A.Nabeeh, and M. Abouhawwash, "An Integrated Neutrosophic Regional Management Ranking Method for Agricultural Water Management," Neutrosophic Systems with Applications, vol. 1, no. SE-Articles, pp. 22–28, Jan. 2023.

[21] Jesus Estupiñan Rcardo,Maikel Leyva Vázquez, Neutrosophic Multicriteria Methods for the Selection of Sustainable Alternative Materials in Concrete Design, American Journal of Business and Operations Research, Vol. 6 , No. 2 , (2022) : 28-38 (Doi : https://doi.org/10.54216/AJBOR.060203)

[22 I. Sahmutoglu, A. Taskin, and E. Ayyildiz, "Assembly area risk assessment methodology for post-flood evacuation by integrated neutrosophic AHP-CODAS," Natural Hazards, vol. 116, no. 1, pp. 1071–1103, 2023.]

Received: July 5, 2023. Accepted: Nov 20, 2023