Received: 26 September 2022 | Revised: 31 May 2023 | Accepted: 12 July 2023

DOI: 10.1002/ett.4841

RESEARCH ARTICLE

WILEY

A comparative analysis of multi-criteria decision methods for secure beacon selection in vehicular platoons

Sean Joe Taylor[1] | **Farhan Ahmad**[2] | **Hoang Nga Nguyen**[3] | **Siraj Ahmed Shaikh**[3] | **Jeremy Bryans**[1] | **Charles E. Wartnaby**[4]

[1]Systems Security Group, Centre for Future Transport and Cities (CFTC), Coventry University, Coventry, UK

[2]Expleo Group, Derby, UK

[3]Systems Security Group (SSG), Department of Computer Science, Swansea University, Swansea, UK

[4]Applus IDIADA, Cambridge, UK

Correspondence
Sean Joe Taylor, Systems Security Group, Centre for Future Transport and Cities (CFTC), Coventry University, Coventry, UK.
Email: taylo314@uni.coventry.ac.uk

Abstract

Vehicle platoons are a novel transportation technology which not only aims to ensure traffic safety but also create a positive impact on the environment by producing low CO_2 emissions. Vehicle platoons rely heavily on wireless communication to ensure that vehicles (leader and members) moving at high speed can keep close formation by exchanging beacons containing significant, authentic and accurate information. However, the presence of malicious attackers launching different attacks such as false data injection (FDI) can compromise the security of vehicle platoons by tampering with the beacons. Therefore, to avoid FDI attacks, we relied on multi-criteria decision methods (MCDM)-based methods in order to select the optimum beacon to share authentic and accurate information with the member vehicles. In this study, three MCDM methods including weighted sum model, technique for order of preference by similarity to ideal solution and preference ranking organization method for enrichment of evaluations (PROMETHEE-II) are studied and compared with the aim to enable the platoons to select the optimum beacon for communication. We performed extensive simulations to evaluate the performance of these methods in the presence of three FDI attacker models from four different aspects, that is, safety, stability, environmental, and cyber security. Our results demonstrate that MCDM-based methods can increase network efficiency, but at the cost of a trade-off between safety and cyber security.

1 | INTRODUCTION

1.1 | Motivation

Vehicular platooning is an emerging connected and automated vehicle (CAV) technology which assists drivers by enabling vehicles to travel in a dense and close formation using wireless communications.[1] By driving in platoons, drivers will see a wide range of benefits, including enhanced road safety, reduced traffic congestion, reduced fuel consumption and hence creating a positive impact on the environment by producing lower carbon dioxide (CO_2) emissions.[2,3] Furthermore, in utilizing wireless communications between vehicles via Vehicle-to-Vehicle (V2V) communications in the formation, vehicles can enter semi-autonomous or autonomous driving modes, reducing the driver's workload by automating driving tasks such as vehicle speed and position.[4] Such technologies enable vehicles to operate safely when keeping minimal inter-vehicle distance at both low and high speeds.[2,5] In platooning, the platoon's first vehicle (called the lead vehicle) is normally operated by a human driver, while the following platooning vehicles (called member vehicles) are operated autonomously using behavior commands which are transmitted and shared from the lead vehicle.[6-8] Figure 1 shows a simple platoon application on a multi-lane roadway where the green arrows show the leader to all and the blue arrows show the vehicle to vehicle behind communications.

To maintain their platoon formation and cohesion, all vehicles that are part of a platoon must transmit sensitive information, including *speed*, *acceleration*, *location*, *vehicle ID*, and *time* via beacons at regular intervals.[9-12] Like all wireless communications, V2V messages between platooning vehicles are vulnerable to cyber attacks, which can modify the behavior of one or more vehicles by injecting malicious beacons. This results in a wide range of cyber attacks on the platoons such as false data injection (FDI),[13] Denial-of-Service (DoS)[14] or Sybil attacks,[7] to name a few. A little tampering with the information in the beacon can lead to significant disruption to platooning vehicles,[15] which often travel at high speeds with minimal inter-vehicle distance.[2]

FDI attacks are high-risk attacks in vehicular platoons as the member vehicles rely highly on the beacons to maintain their positions in autonomous mode. A slight change in one beacon component can destabilize the whole platoon.[5,15,16] To avoid the risk of collision, platooning vehicles may disband as the situation is considered unsafe and therefore lose all benefits from platooning for both platooning and non-platooning vehicles.[5,15] Current methods of securing platoons from FDI attacks from non-member vehicles heavily rely on public and private key infrastructure. As such, there is a multitude of research describing various ways that public and private keys can be kept secure from potential attackers.[6,17-22] Here we propose an auxiliary method to help platoons maintain safe driving formations even if the attacker has broken the member-to-member public and private key infrastructure.

Multiple-criteria decision-making (MCDM), also known as multiple-criteria decision analysis, describes various methods used to make decisions in an intelligent manner. MCDM is used extensively in various disciplines including business, industries, construction and cyber security.[23-26] MCDM can handle numerical and non-numerical information, even with conflicting criteria, to identify the best choice based on available information. As such, this can be applied to the beacons used by platooning vehicles to prevent false information from being used by platooning vehicles. By comparing the most recent beacon to the last beacon, the leader's beacon and a predicted beacon—before the platoon controller uses the beacon—a false beacon should be ignored before it has the chance to be used by the vehicle and therefore disrupt the platoon. This article compares several MCDM which enable the platoon vehicles to identify and select real beacons from fake beacons when under FDI attacks, thus preventing an attacker from being able to influence the platoon's behavior. To this end, three MCDM methods, namely *weighted sum model (WSM)*,[25] *technique for order of preference by similarity to ideal solution (TOPSIS)*[27] and *preference ranking organization method for enrichment of evaluations (PROMETHEE II)*[28] are studied, implemented and compared in order to evaluate the efficiency of the vehicular platoons to select best beacon when under FDI attacks. To this end, this article aims to evaluate each MCDM method from four aspects: safety, stability, environmental, and cyber security. Next, a comparison is provided to understand which MCDM method is able to detect and select true beacons in the presence of FDI attacks.

1.2 | Article contributions

The major contributions of our study are:

1. To propose a novel method to select true beacons for vehicular platoons using three MCDM (WSM, TOPSIS, and PROMETHEE II) methods in presence of FDI attacks.
2. To provide a comparative study for beacon selection using three MCDM methods within vehicular platoons in presence of three FDI attack models.

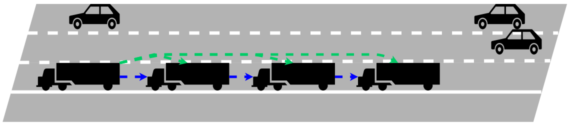


FIGURE 1 Simple platoon application on a multi-lane road.

3. To rigorously evaluate the performance of three MCDM methods from four significant aspects including *safety*, *stability*, *environmental*, and *cyber security*.
4. To discuss and argue which method is applicable and efficient in detecting true beacons within vehicular platoons in the presence of various FDI attacks.

1.3 | Article organization

The rest of the article is organized as follows: Section 2 discusses related work to mitigate FDI attacks in vehicular platoons and the use of MCDM in V2V communications. Section 3 introduces three techniques of MCDM: WSM, TOPSIS, and PROMETHEE-II, and how they are applied to platoons as a security method. Section 4 provides a comprehensive description of the simulation environment used to evaluate the platoon against the three attack models, while Section 5 provides the results of the simulations from four aspects, that is, *safety*, *stability*, *environmental*, and *cyber security*. Next, Section 6 provides a detailed comparison of these implemented methods and provides suggestions for the best method to be implemented in vehicular platoons to prevent FDI attacks. Finally, Section 7 closes out the article.

2 | RELATED WORK

The world is on the way to introducing vehicles on the roads that are more connected and autonomous to make transportation safer, faster and smarter. However, these wirelessly connected vehicles pose various cyber security issues, which need to be addressed to protect us from various security attacks.[29] Public key infrastructure (PKI) is a significant research topic in securing CAV vehicles such as vehicle platoons from malicious attacks.[17,18] Extensive research exists in the literature on securely passing keys between vehicles when connecting in an ad-hoc method in vehicular platoons. Li et al. proposed a method which uses quantized fading channel randomness[18] to create keys in a secure mechanism. The proposed method uses multi-path fading to create unique keys for vehicles during communication. The main advantage of this approach is that it prevents an eavesdropper from obtaining the same key due to the fact that the multi-path fading of the channel to the malicious node is different to that of the legitimate member. However, this method requires additional equipment to be mounted on the vehicle, which is the main drawback of this approach. Lai et al., on the other hand proposes a method to rely on adjacent infrastructure such as road side units (RSU's) to facilitate the assignment of a key between vehicles. In this proposed model, vehicles communicate with an RSU[17] to form and join a platoon. Based on the recommendation of the RSU, vehicles can only communicate if they have received keys from the RSU. Using this approach provides two main advantages: it (1) provides significant control to trusted authorities in managing the keys for platooning vehicles, and (2) no additional equipment needs to be mounted on the platooning vehicles to exchange keys. However, the vehicles need to be within the range of the RSU in order to form the platoon and exchange keys, which makes it the major weakness of this approach. Furthermore, RSU's are vulnerable to physical damage and failure as well as cyber-attack,[30] which can create additional problems for vehicles wishing to create or join the platoon.

In addition to PKI, some studies have focused on methods to prevent damaging platoon behavior from disrupting a platoon. Such methods often work by identifying behavior patterns using control algorithms such as the Lyapunov–Krasovskii approach, which could destabilize a platoon, leading to a collision or loss of platoon efficiency.[6] These methods rely on sensor data and information from other platoon members to identify and suppress behaviors considered damaging to the platoon.[6,19] Other methods use alternative wireless communication methods, such as visible light communications (VLC) as a secondary communication method proposed by Ucar et al.[20] The main advantage of these methods is that the platoon can be secured from unpredictable behavior without any additional external infrastructure such as RSU's. However, this security approach comes at the cost of an unavoidable delay in detecting and preventing damaging behavior, which is the main drawback of these approaches.

Multi-criteria decision methods (MCDM) have been used in transportation previously in the literature with the aim of addressing routing issues. For instance, MCDM has been used in vehicle ad hoc networks (VANET's)[25] due to (i) their ability to use multiple different attributes to calculate the best possible result, and (ii) their ease of scaling to larger networks.[31] WSM is proposed to be used in the routing protocol proposed by Elgaroui et al. for its robustness, scalability and simplicity in identifying optimum routes using the received signal strength indication (RSSI).[25] The goal of using WSM using RSSI is to create a more effective routing mechanism which can be employed for V2V communications within VANET's. On the other hand, Nandy et al.[28] proposed to use PROMETHEE-II in a group-based communication in VANET's for the selection of a cluster head, which then communicates with the other nodes to exchange information.

TABLE 1 FDI attack prevention methods, their advantages and disadvantages.

		FDI prevention method					
Article	Year	PKI	IDM	Block chain	MCDM	Advantages	Disadvantages
17, 17	2016	✓				No additional on vehicle equipment needed	Reliant on RSU's to distribute keys
20	2018		✓			Uses visible light communications to aid V2V	Need for additional equipment to be mounted to vehicles and time to compare messages, creating delay
6	2018		✓			Proven for vehicle platoons	There is still some disruption to the platoon
19	2019		✓			Simple to implement	Heavily reliant on information from other vehicles
18	2019	✓				No transmission of keys between members	Additional specialist equipment is needed
21	2020			✓		Extremely robust and difficult to fake.	Only applied to the leader vehicle.
22	2022	✓				Able to authenticate both the vehicle and the message extending at a reduced computational cost than other methods.	Currently only protects platoons when a vehicle joins the platoon.
Current study	2023				✓	No delay in identifying and preventing, damaging behavior and no additional equipment needed	Needing a truthful and responsible lead vehicle.

TOPSIS-based methods have also been used in VANET routing protocols to improve transmission rates and reduce computing times.[26,32] Furthermore, these methods can be used to rank and select channels to transmit messages to other vehicles. Moreover, these methods can help to analyse the packets. These aspects play a vital role in ensuring that information is transmitted with minimum possible delay and accurately to all appropriate recipients in a VANET, which ultimately improves the reliability of the network.[26] In the study by Arif et al.,[26] TOPSIS is compared against other methods including MOORA and SAW. These methods were evaluated for random packet loss and ranked-based channel selection aspects. In doing so, it is identified that using TOPSIS can address a range of societal and environmental issues by improving channel selection within a cognitive radio (CR) Enabled Internet on Vehicle (CR-IoV).[26]

Various security methods have been proposed using PKI and intrusion detection methods (IDM) to secure vehicular platoons. Moreover, MCDM methods have not been used to secure vehicle platoon communications from attacks. As vehicular platoons have their specific characteristics compared to VANET's due to the fact that platoons are less dynamic and generally transmit more sensitive information. Therefore, implementing traditional security methods from VANET's cannot be employed directly in vehicular platoons. This study fills this gap by providing a comparative study between three MCDM methods (i.e., WSM, TOPSIS, and PROMETHEE-II) for ensuring secure beacon selection in vehicular platoons. Table 1 compares various security solutions in VANET's and vehicular platoons along with their advantages and disadvantages. In the next section, we provide details of the three MCDM methods and its implementation in the vehicular platoons.

3 | SYSTEM MODEL

3.1 | System model

In order to prevent FDI attacks in vehicular platoons, the vehicles need to select the optimum (i.e., genuine) beacon involving two steps: (i) beacon prediction, and (ii) beacon selection, a system model is shown in Figure 2.

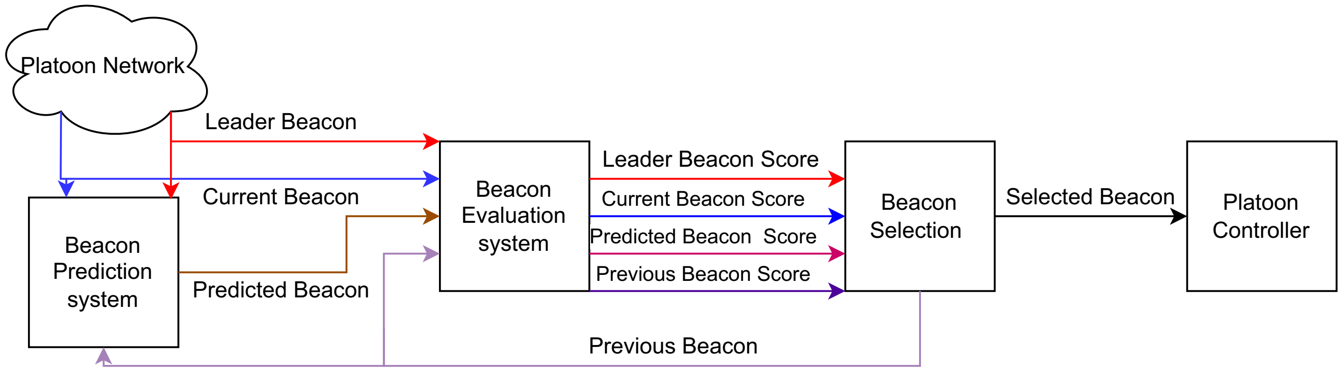


FIGURE 2 A simple diagram outlining the beacon prediction and beacon selection.

3.1.1 | Beacon prediction

The predicted beacon system receives three different types of beacons, that is, (i) a previously received beacon, (ii) a current beacon, and (iii) a leader beacon. The first step is taking the clock time in seconds, of the platooning vehicle, rounding it to two significant figures, and subtracting 0.01 to provide an estimated time for when the beacon would have been created; this value is used as the time component of the predicted beacon. The speed component of the predicted beacon is the reported vehicle speed in the leader's beacon. The leader's speed is used as it is the ideal speed of the platoon at any given time to maintain steady-state platooning. Finally, the acceleration and location components of the predicted beacon come from the current beacon. The use of the current beacon information does enable the attacker to be able to influence the predicted beacon; however, in this article's simulations, there is little to no impact on the platoon formation by doing this. Therefore, the leader and previous beacons are not used, as this will negatively impact the platoon's formation. This information is significantly different from the current and would destabilize the platoon if used.

3.1.2 | Beacon selection

Once the beacon is predicted, the next step is to select the optimum beacon with highest score. In this article, we utilize MCDM methods in order to identify optimum beacon to be used by the platoon controllers. MCDM calculations produce a numerical value for each choice, representing its preference over the other choices. In this application, the choices are the leader beacon (LB), current beacon (CB), previous beacon (PastB), and predicted beacon (PreB). For the three methods of MCDM presented in this article, the best choice is the one with the highest score. Therefore, the vehicle must compare the MCDM scores to select the most significant one. The vehicles are biased towards the LB and CB in cases where scores are the same. The LB is used when LB is equal to any other beacon, as this will maintain the vehicle's safe positioning in the platoon when using the co-operative adaptive cruise control (CACC) platoon controller. The CB is used when CB is equal to PastB or PreB as using CB is using the most up-to-date information to give maximum accuracy in vehicle positioning as it is possible for multiple values to very rarely equal the PastB or PreB based on the interaction with the MCDM. In addition, there are three other conditions that the beacon must also satisfy in order to be selected to prevent unsafe platooning. The first is that the beacon's time stamp must be less than the current time; this prevents inaccurate time stamps from creating problems for the CACC controller. The next component is that the positive speed must not exceed +10 mps more than the leader's as this helps to maintain platoon stability during acceleration. Finally, according to ENSEMBLE project, acceleration and speed must not be lower than −3.5 mps for normal vehicle deceleration.[33] If the best beacon does not align with the above conditions or if no beacon is selected for any reason, the leader's beacon is loaded to maintain the momentary loss of usable beacons. By doing this the vehicle is able to maintain safe platooning even in this worst case scenario. In the next section, we provide details of the three MCDM methods which are implemented within the vehicular platoons.

3.2 | Multi-criteria decision methods in vehicular platoons

MCDM describes various methods used to make decisions and is used extensively in various disciplines, including industrial internet of things[34] and cyber security.[35] MCDM can handle numerical and non-numerical information and often conflicting criteria to identify the best choice based on available information.

For example, MCDM methods can improve a platoon's resistance to false beacon information by comparing the new (current) beacon with the last received leader's beacon and a self-made predicted beacon. By using MCDM to compare the received beacons before using them in the platoon controller to filter out potential false beacons, the vehicles will be able to maintain ideal inter-vehicle distance and platoon stability better. In MCDM, the choices are the different options being considered, and the attributes are a common set of characteristics of each choice that may or may not be favorable. MCDM can use the attributes to identify the best possible alternative. When applied to vehicle platoon beacons, the beacon is the choice, and the elements in the beacon are the *attributes*. The attributes are the elements within a beacon that are responsible for the platoon behavior and are: speed (s), acceleration (a), controller acceleration (ca), X position (XPos), Y position (YPos), and time (t) and summarized in Table 2.

Each attribute also requires a weighting (w) and is calculated using the best-worst method[36] where the weighted sum equals one. The most important and least important components are picked for the best-worst method, and all other components are rated against them. The most important value is the time, and the least important is the controller acceleration and this due to the way that the CACC interprets and uses the components of the beacon in its navigation. Garlichs et al.,[37] state that acceleration and speed were the most influential components of a beacon when determining platoon member behavior as these two values control the longitudinal position of a platooning vehicle. When using MCDM time is the most influential, giving strength to the most up-to-date beacon, the speed the second most-weighted attribute. The controller acceleration is not involved directly with vehicle positioning and is used to tell the CACC the target acceleration of the preceding vehicle and is therefore the least influential attribute. When each attribute is normalized, it becomes signless and thus enabling the fair comparison of all attributes. This article considered the following three MCDM methods to select the best beacon for vehicular platoons.

3.2.1 | Weighted sum model

WSM is a simple but effective MCDM method which can be used to evaluate alternatives and can be easily scaled to suit the number of choices and criteria being compared. WSM works as each criterion is assigned weight before adding all criteria together for a single choice to give an overall score called the WSM score. The largest WSM score is the best choice.

The first step is to take all four beacons, LB, CB, PastB, and PreB in order to create Table 3 using the real data values. The next step is to normalize the values which is done in two ways. First, if the attribute is more beneficial when greater than zero, it is called a *benefit* attribute. Equation (1) shows how to normalize a beacon component (such as speed (s)).

TABLE 2 Beacon characteristics.

Platoon beacon characteristics	Details	Acronym
Beacon choices	Leader beacon	LB
	Current beacon	CB
	Previous beacon	PastB
	Predicted beacon	PreB
Beacon attributes	Speed	s
	Acceleration	a
	Controller acceleration	ca
	X position	XPos
	Y position	YPos
	Time	t

TABLE 3 Beacon attributes table.

Beacon	s (mps)	a (mps^2)	ca (mps^2)	XPos (m)	YPos (m)	t (s)
LB	22.22	0.001	0.002	100	1	1.45
CB	22.22	8.80E−05	0.002	74	1	1.48
PreB	22.22	8.80E−05	0.002	74	1	1.47
PastB	22.22	2.81E−05	0.002	70	1	1.22

$$x_{ij} = \left(\frac{1}{X_{LB_s}} + \frac{1}{X_{CB_s}} + \frac{1}{X_{PreB_s}} + \frac{1}{X_{PastB_s}}\right)/X_s. \tag{1}$$

If the attribute is more beneficial when equal to zero, then it is a *cost* attribute which is calculated using Equation (2) using time (t) as an example.

$$x_{ij} = (X_{LB_t} + X_{CB_t} + X_{PreB_t} + X_{PastB_t})/X_t. \tag{2}$$

In both Equations (1) and (2), x_{ij} is the normalized attribute value, and X is the real value of the attribute. For platoon beacons, the cost attributes are s, a, and ca as they improve braking performance, while *XPos*, *YPos*, and t are classified as benefit attributes. *XPos* and *YPos* are benefit attributes as they ensure improvement in the stability of the platoon. Time is also a beneficial attribute to give greater influence to the most recent beacon. After normalizing each attribute, the next step is multiplying the attribute weighting by the normalized attribute value where w is the weighting of the attribute. Finally, each attribute in each beacon is added to produce the WSM score. Table 4 provides an example of calculating WSM score for all the choices. CB will be selected from this example as it achieved the highest WSM score.

3.2.2 | Technique for order of preference by similarity to ideal solution

Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) was originally developed by Ching-Lai Hwang, and Kwangsun Yoon in 1981.[38] The concept of TOPSIS is that the chosen alternative should have the shortest geometric distance to the positive ideal solution and be furthest from the negative ideal solution. To achieve this, an ideal best and an ideal worst are selected for each attribute for each choice. As such, each choice compares attributes with each other, with the best becoming the ideal best and the worst becoming the ideal worst.

TOPSIS starts by creating Table 3. The next step is to normalize the TOPSIS values using Equation (3). For each attribute (X), the normalization equation is the same regardless of if the attribute is a cost or benefit. Next, the normalized attributes are multiplied by the attribute weighting w.

$$x_{ij} = \frac{X}{\sqrt{\sum_{j=1}^{n} X^2}}. \tag{3}$$

This step involves the best and worst for each attribute to be identified. The ideal best is the most advantageous attribute, for the example in Table 5 for a the ideal best value is 0.058 (LB_a). The ideal worst is the least advantageous, for

TABLE 4 Example of WSM for selecting, all values are normalized.

	s	a	ca	XPos	YPos	t	WSM score
Beacon	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$	P_i
LB	0.25	0.031	0.267	0.314	0.25	0.258	0.251
CB	0.25	0.419	0.244	0.233	0.25	0.263	0.262
PastB	0.25	0.131	0.244	0.233	0.25	0.262	0.245
PreB	0.25	0.419	0.244	0.22	0.25	0.217	0.242

Note: Unit before normalization: s (mps), a (mps^2), ca (mps^2), XPos (m), YPos (m), and t (s).

TABLE 5 TOPSIS complete table, all values are normalized.

	s	a	ca	XPos	YPos	t	S_i^+	S_i^-	Performance score
Beacon	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$	$x_{ij} * w$			P_i
LB	0.114	0.058	0.013	0.097	0.068	0.201	0.004	0.069	0.941
CB	0.114	0.004	0.014	0.072	0.068	0.206	0.059	0.036	0.380
PastB	0.114	0.014	0.014	0.072	0.068	0.204	0.051	0.036	0.415
PreB	0.114	0.004	0.014	0.068	0.068	0.169	0.071	0.001	0.016
Best	0.114	0.058	0.014	0.097	0.068	0.206			
Worst	0.114	0.004	0.013	0.068	0.068	0.169			

Note: Unit before normalization: s (mps), a (mps^2), ca (mps^2), XPos (m), YPos (m), and t (s).

example in Table 5 for a the ideal worst value is 0.004 (CB_a and $PreB_a$). Table 5 shows this step implemented using the example. The ideal best and worst are needed to be able to calculate the ideal best Euclidean distance (S_i^+) and the ideal worst Euclidean distance (S_i^-). The equation for the ideal best Euclidean distance is shown in Equation (4) where V_{ij} is the weighted normalized value, and V_j^+ is the ideal best attribute.

$$S_i^+ = \left[\sum_{j=i}^{m} (V_{ij} - V_j^+)^2\right]^{0.5}. \tag{4}$$

The equation for the ideal worst Euclidean distance is shown in Equation (5) where V_{ij} is the weighted normalized value, and V_j^- is the ideal worst attribute.

$$S_i^- = \left[\sum_{j=i}^{m} (V_{ij} - V_j^-)^2\right]^{0.5}. \tag{5}$$

With the Euclidian distances calculated using Equations (4) and (5) for each beacon. Finally calculating the performance score (P_i). The largest performance score is the best beacon to be used for the CACC, and in this example, would be the leader beacon.

$$P_i = \frac{S_i^-}{S_j^+ + S_j^-}. \tag{6}$$

3.2.3 | Preference ranking organization method for enrichment of evaluations

Preference ranking organization method for enrichment of evaluations (PROMETHEE) works to present the choice that best fits the goal. As such, this behavior could make it advantageous for use in securing vehicle platoons beacons against FDI attacks. The first step is to construct a decision matrix shown in Table 3. For each attribute the maximum ($max(x_{ij})$) value and the minimum ($\min(x_{ij})$) value are identified. Then the decision matrix needs to be normalized for beneficial attributes as shown in Equation (7) and cost attributes in Equation (8). Where R_{ij}^+ is the normalized benefit value, R_{ij}^- is the normalized cost value and x_{ij} is the initial value, producing Table 6.

$$R_{ij}^+ = \frac{[x_{ij} - \min(x_{ij})]}{[\max(x_{ij}) - \min(x_{ij})]}, \tag{7}$$

$$R_{ij}^- = \frac{[\max(x_{ij}) - x_{ij}]}{[\max(x_{ij}) - \min(x_{ij})]}. \tag{8}$$

TABLE 6 PROMETHEE II example after normalizing the values.

Beacon	s	a	ca	XPos	YPos	t
LB	0	0	1	1	0	1.45
CB	0	0.949	0	0.133	0	1.48
PreB	0	0.949	0	0.133	0	0.962
PastB	0	1	0	0	0	0

Note: Unit before normalization: s (mps), a (mps^2), ca (mps^2), XPos (m), YPos (m), and t (s).

TABLE 7 Example of the first four rows for calculating the evaluative differences of *i*th alternative concerning all other alternatives.

Beacon	s	a	ca	XPos	YPos	t
LB-CB	LB_s-CB_s	LB_a-CB_a	LB_{ca}-CB_{ca}	LB_{XPos}-CB_{XPos}	LB_{YPos}-CB_{YPos}	LB_t-CB_t
LB-PastB	LB_s-PastB_s	LB_a-PastB_a	LB_{ca}-PastB_{ca}	LB_{XPos}-PastB_{XPos}	LB_{YPos}-PastB_{YPos}	LB_t-PastB_t
LB-PreB	LB_s-PreB_s	LB_a-PreB_a	LB_{ca}-PreB_{ca}	LB_{XPos}-PreB_{XPos}	LB_{YPos}-PreB_{YPos}	LB_t-PreB_t
CB-LB	CB_s-LB_s	CB_a-LB_a	CB_ca-LB_ca	CB_XPos-LB_XPos	CB_YPos-LB_YPos	CB_t-LB_t

TABLE 8 Example showing the evaluative differences of *i*th alternative concerning all other alternatives ($a - b$) and then the preference function (R_{aj}).

	s		a		ca		XPos		YPos		t	
Beacon	$a-b$	R_{aj}	$a-b$	R_{aj}	$a-b$	R_{aj}	$a-b$	R_{aj}	$a-b$	R_{aj}	$a-b$	R_{aj}
LB-CB	0	0	−0.949	0	1	1	0.867	0.867	0	0	−0.115	0
LB-PastB	0	0	−1	0	1	1	1	1	0	0	0.885	0.885
LB-PreB	0	0	−0.949	0	1	1	0.867	0.867	0	0	−0.077	0
CB-LB	0	0	0.949	0.949	−1	0	−0.867	0	0	0	0.115	0.115
CB-PastB	0	0	−0.051	0	0	0	0.133	0.133	0	0	1	1
CB-PreB	0	0	0	0	0	0	0	0	0	0	0.038	0.038
PastB-LB	0	0	1	1	−1	0	−1	0	0	0	−0.885	0
Past-CB	0	0	0.051	0.051	0	0	−0.133	0	0	0	−1	0
PastB-PreB	0	0	0.051	0.051	0	0	−0.133	0	0	0	−0.962	0
PreB-LB	0	0	0.949	0.949	−1	0	−0.867	0	0	0	0.077	0.077
PreB-CB	0	0	0	0	0	0	0	0	0	0	−0.038	0
PreB-PastB	0	0	−0.051	0	0	0	0.133	0.133	0	0	0.962	0.962

The next step is to calculate the evaluative differences of *i*th alternative concerning all other alternatives. Each message and its attributes are subtracted from another message to give $a - b$, which is the evaluative differences of *i*th alternative concerning all other alternatives. The first four rows are shown algebraically in Table 7. The matrix is filled when all choices are compared directly against each other, as shown in Table 8. Once the matrix is created, the next step is to calculate the preference function, $P_j(a, b)$, which can be calculated using Equations (9) and (10). Where R_{aj} is the resulting difference between two attributes shown in Table 8.

$$P_{j(a,b)} = 0 \ if \ R_{aj} \leq 0, \tag{9}$$

$$P_{j(a,b)} = (R_{aj}) \ if \ R_{aj} > 0. \tag{10}$$

TABLE 9 Example of aggregated preference function matrix.

	Leader	Current	Previous	Predicted
Leader	-	LB-CB	LB-PastB	LB-PreB
Current	CB-LB	-	CB-PastB	CB-PreB
Previous	PastB-LB	PastB-CB	-	PastB-PreB
Predicted	PreB-LB	PreB-CB	PreB-PastB	-

TABLE 10 The entering and leaving flows for the example as well as the net outranking frow.

	Leader	Current	Previous	Predicted	Leaving flow	Net outranking flow
Leader	-	0.163024139	0.53021643	0.163024139	0.285421569	−0.12805663
Current	0.175109859	-	0.412366202	0.008763135	0.198746399	−0.14207265
Predicted	0.136933057	0.006997108	-	0.006997108	0.050309091	0.396321197
Previous	0.160051889	0	0.397308232	-	0.185786707	−0.12619191
Entering flow	0.157364935	0.056673749	0.446630288	0.059594794		

All values equal to or less than zero be changed to zero and all values greater than zero unchanged. The following step is to calculate the aggregated preference function $\pi(a,b)$ according to Equation (11) where w is the weights as used before.

$$\pi(a,b) = \frac{\left[\sum_{j=1}^{n} w_j P_j(a,b)\right]}{\sum_{j=1}^{n} w_j}. \tag{11}$$

The aggregated preference functions for each comparison are then used to create a new matrix as shown in Table 9 with the worked example shown in Equation (13).

The next step is to calculate the *entering* and *leaving* flow. The alternative's entering (negative) flow is the average of each column, and the leaving (positive) flow for the alternative is the average of each row. Equation (12) is an example of how the entering flow is calculated using the LB and Equation (13) is an example for how the leaving flow is calculated using LB. Where E_{LB} is the entering flow for the LB and L_{LB} is the leaving flow for the LB, the other beacons are calculated the same way.

$$E_{LB} = (CB - LB) + (PastB - LB) + (PreB - LB), \tag{12}$$

$$L_{LB} = (LB - CB) + (LB - PastB) + (LB - PreB). \tag{13}$$

The final step is to calculate the net outranking flow (P_i) for each alternative, which is achieved by subtracting the entering flow from the leaving flow for each alternative Equation (14).

$$P_i = E - L, \tag{14}$$

where E is the entering flow and L is the leaving flow resulting in Table 10. The best beacon identified by PROMETHEE II using this example is the predicted beacon (PreB) to be used by the CACC.

4 | SIMULATION SETUP

In order to compare the effectiveness of each MCDM method at preventing FDI attacks on vehicle platoons, the open source simulator called plexe is used.[39] Plexe is a platooning extension to the Veins[40] simulation environment built using OMNET++ network simulator[41] and integrated with SUMO.[42] With Veins handling the vehicle nodes and their behavior, OMNET++ simulates the wireless communications network while SUMO provides road network information and another graphical user interface.

The platoon is simulated in a map of (650 × 250) km where all vehicles operate on a multi-lane road at maximum speed of 80 kph. In this study, single platoon consisting of eight vehicles is modeled with one leader and seven member vehicles. Moreover, once the platoon is completed, human-driven attacker vehicles are introduced in the network which perform FDI attacks. The platoons are attacked several times where the number of attackers or victim vehicles increases which is done to show the full impact of the FDI attacks on the platoon for each MCDM. Further simulation parameters are listed in Table 11.

4.1 | Platoon model

The platoon model used makes several assumptions about the platooning vehicles. First, the leader vehicle always gives accurate information in its beacon, and the attacker cannot pretend to be the leader. All platooning vehicles use CACC as described in the California path project[43] as the platoon controller. The platoon is formed, and no vehicles are joining or leaving the platoon during the simulation. There are no faulty sensors or other equipment on the platooning vehicles. All member vehicles use MCDM to select the beacon sent to their platoon controller from the platoon network.

4.2 | Attacker model

The attacker models are discussed in detail here, along with their assumptions. The first assumption is that the attacker cannot spoof the leader's messages but can spoof any platoon member. The attacker can create beacons that are recognizable to the platoon and that the attacker has broken PKI for the member vehicles. The attacker, however, is not a member of the platoon. The attacker always targets as close to the leader as possible, giving the most opportunity to destabilize the

TABLE 11 Simulation parameters.

Parameters	Value
Simulation time (s)	1000 s
Simulation area (km × km)	650 km × 250 km
Platoon controller	CACC
Total number of vehicles in platoons	8
Human-driven vehicle (attacker)	1-6
MAC protocol	IEEE 802.11p
Network protocol	WAVE
Radio propagation model	Two-ray interference
Packet size	200 bits
Ideal inter-vehicle distance	15 m[2]
Platooning vehicle speed	22.2222 mps (80 kph)
Message bit rate	6 Mbps
Packet loss rate	0.2
w_s	0.227841516
w_a	0.059835086
$w_c a$	0.027440775
$w_X Pos$	0.156442343
$w_Y Pos$	0.136933057
w_t	0.391507223

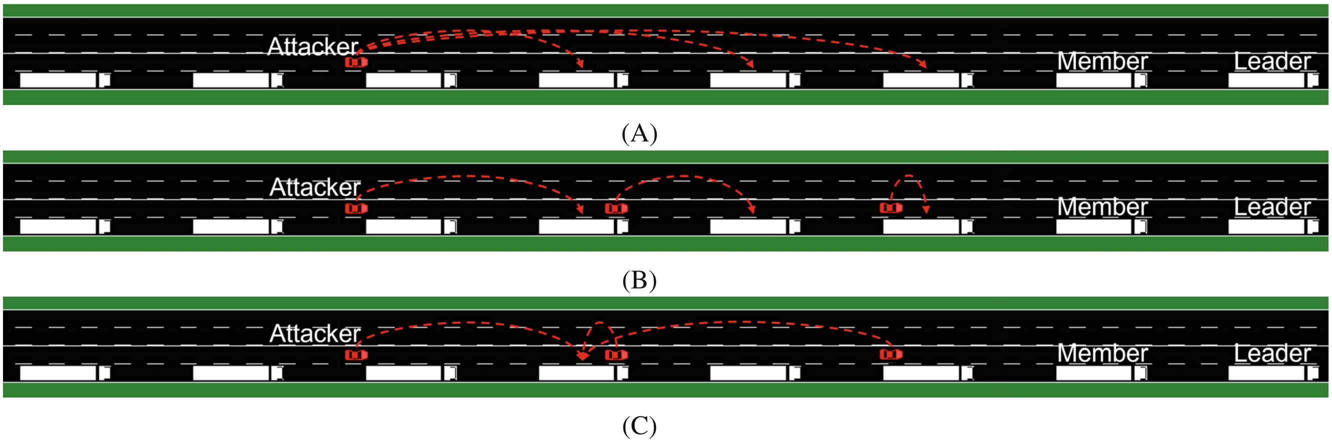


FIGURE 3 The attack scenarios used to test MCDM as a security method in platoons. (A) Single attacker attacking multiple platoon members. (B) Multiple attackers attacking multiple member. (C) Multiple attackers attacking a single member.

platoon. Finally, the beacon injected in by the attacker will have a vehicle speed of 0.5 mps more than the platoon's speed. There are three attack models that are considered; *single attacker multiple victims*, *multiple attackers multiple victims*, and *multiple attackers single victim*.

4.2.1 | Single attacker multiple victims

In this attack model, a single attacker attacks the platoon as shown in Figure 3A. The attacker will switch between each vehicle it is attacking to avoid detection. When the simulation is run, the attacker will attack between 1 and 6 of the platooning member vehicles. Six is the maximum number the attacker can attack as, at this point, there are no more member vehicles it can attack. This attack aims to lower the chances of being identified by spoofing the ID of multiple different member vehicles and not concentrating on a single vehicle. As such, the defensive method used by the platoon must react very quickly to prevent the attacker from negatively impacting the platoon.

4.2.2 | Multiple attackers multiple victims

For the multiple attackers attacking multiple vehicles shown in Figure 3B, the attackers work co-operatively to attack multiple members simultaneously, where each attacker focuses on a single member that only it attacks. There are between one and six attackers. This is due to there being only six member vehicles that can be attacked. This attack aims to compromise member-to-member communications in the platoon between multiple members simultaneously. To overcome this, the defense method used must be able to prevent the fake beacons from being injected into the platoon network by the attackers without obstructing the use of the true beacons.

4.2.3 | Multiple attackers single victim

The third attack model is where multiple vehicles work co-operatively to attack a single platoon member and is shown in Figure 3C. As before, there are between one and six attackers attacking the platoon. Six is the maximum number of attackers first to keep uniformity with the other two attack models but also that the overall behavioral patterns are also clearly shown. In this attack, the attackers put all their effort into attacking a single vehicle; therefore, any defense method needs to be strong and robust to prevent it from being overwhelmed in such attacks.

5 | RESULTS

The results are presented from four distinct aspects, including safety, stability, environmental, and cyber security.

5.1 | Safety

Given that vehicles in a platoon travel at high speed with minimal inter-vehicle spacing between them, any change to the inter-vehicle distance presents a potential safety problem. Therefore maintaining the ideal inter-vehicle distance is vital to the safety of the platoon and other road users. Figure 4 shows the average inter-vehicle distance maintained by platoon members for three different MCDM methods. The gray line represents the average mean inter-vehicle distance between the vehicles in the platoon for each MCDM method and under each attack model. The average mean inter-vehicle distance of all vehicles in the platoon is ideal. With only PROMETHEE II seeing a slight increase in average inter-vehicle distance, it is negligible at less than 0.02 m. The average maximum and minimum inter-vehicle distances are where WSM and TOPSIS are better than PROMETHEE II as they both have an average maximum inter-vehicle of 0.15 m as a minimum of just less than the ideal but are always less than 0.06 m, while. PROMETHEE II sees the minimum inter-vehicle distance reduced by over 0.5 m and a maximum of more than 0.98 m for single attacker multiple victims attack scenarios and over 1 m for multiple attackers multiple victims and multiple attacker single victim.

When looking directly at the inter-vehicle distances shown in Figures 5–7, the similarity and advantages of WSM and TOPSIS over PROMETHEE II become obvious. The WSM and TOPSIS produce identical inter-vehicle distance traces at the ideal inter-vehicle distance almost throughout apart from an initial slight increase after the vehicles start as the vehicles start slightly closer together than the ideal. While the use of PROMETHEE II overall is better than if there is no MCDM used, there is a significant amount of destabilization initially. During the multiple attacker single victim attack method, it cannot return all vehicles to the ideal inter-vehicle distance. When five attackers are attacking a single target vehicle, then the directly attacked vehicle, vehicle two, will brake significantly at around 7 s, increasing its inter-vehicle distance dramatically. Vehicle three does not respond quickly enough to this and sees it close its inter-vehicle distance between it and vehicle close dramatically to 6.06 m, which has the potential to cause the vehicles to collide if the attack is more severe or there is sudden braking.

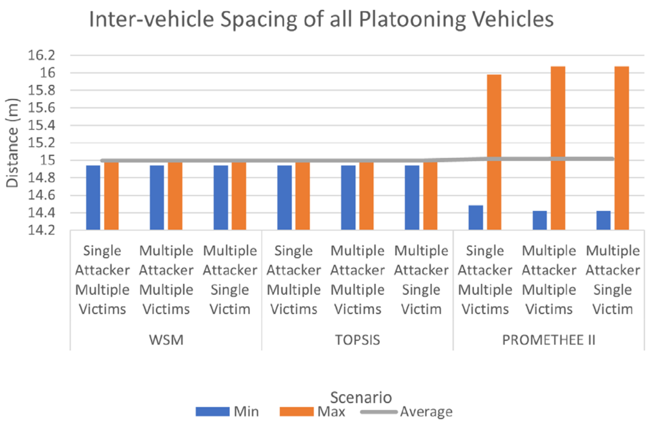
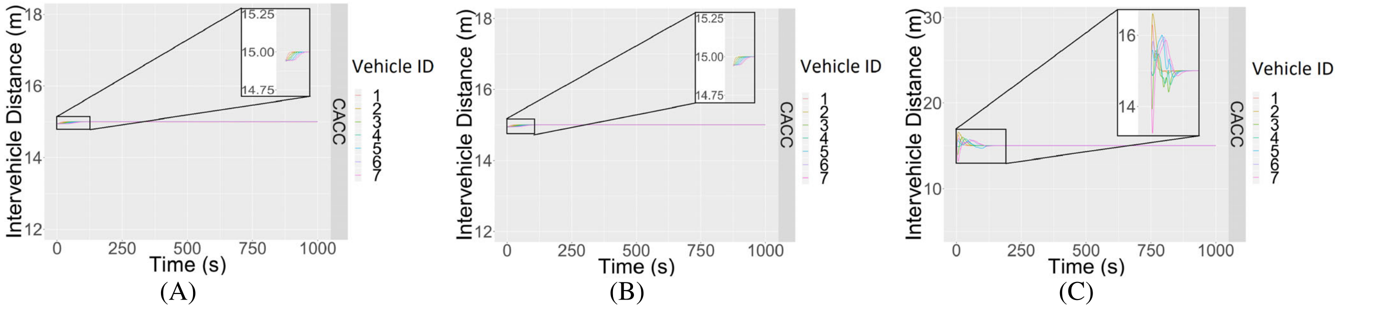


FIGURE 4 The average maximum, minimum inter-vehicle distance and average over all inter-vehicle distance.



(A)
(B)
(C)

FIGURE 5 Single attacker, multiple victims: The inter-vehicle distance of each vehicle when a single attacker attacks four members using (A) WSM, (B) TOPSIS, and (C) PROMETHEE II.

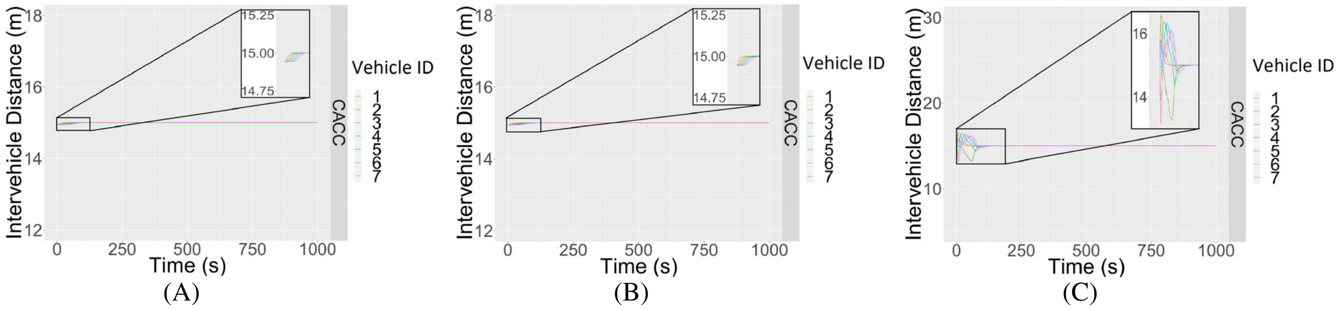


FIGURE 6 Multiple attackers, multiple victims: The inter-vehicle distance of each vehicle when three attackers attack three platooning vehicles using (A) WSM, (B) TOPSIS, and (C) PROMETHEE II.

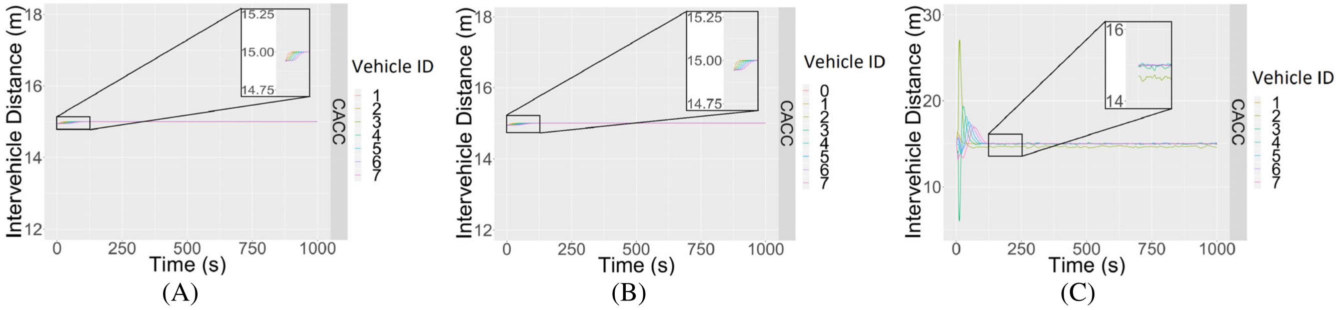


FIGURE 7 Multiple attackers, single victim: The inter-vehicle distance of each vehicle when five attackers attack a single platooning vehicle using (A) WSM, (B) TOPSIS, and (C) PROMETHEE II.

The similarity in behavior shown by WSM and TOPSIS is because of the similarity in their methods that enable both to suppress the FDI attacks in all three attack methods. This is backed up as the inter-vehicle distance trace for each vehicle is very close to the ideal. To achieve this behavior, most, if not all, of the false beacons need to be ignored and not used by the CACC controller. PROMETHEE II, on the other hand, is calculated very differently and, as such, produces very different results. While able to average the inter-vehicle distance to 15 m, it is not as stable as TOPSIS and WSM. This is highlighted in Figure 7C, where the attack heavily impacts the platoon. Therefore it can be inferred that PROMETHEE II cannot prevent false beacons from being sent to the CACC controller; in addition, it prevents some true beacons from being used.

5.2 | Stability

The stability of the platoon is indicated by the speed of each vehicle in the platoon. Under ideal conditions, a platoon's speed should be constant. If the leader makes any speed adjustments, the platoon should respond accordingly and immediately while maintaining the ideal inter-vehicle distance. Figure 8 shows the average mean speed of each vehicle in the platoon in gray, and the average maximum and minimum speeds. The average mean vehicle speed for all three MCDM methods is the same and ideal at 22.222 mps (80 kmph). The maximum and minimum speeds for both WSM and TOPSIS are ideal at 22.222 mps (80 kmph). PROMETHEE II, however, has significant variations in the maximum and minimum vehicle speeds. The average minimum vehicle speed drops to 21.59 mps, which is a significant drop in speed; however, it is not long-term. The maximum vehicle speed is 23.32 mps. The maximum speed is more than what is seen in WSM and TOPSIS, which suggests that PROMETHEE II is less stable than WSM and TOPSIS.

To get a better understanding of how the vehicle's speed is impacted when under FDI attack for the three MCDM methods, Figures 9–11 are used. Looking at the vehicle speeds in more detail, Figures 9A,B–11A,B show near-ideal vehicle speeds achieved via WSM and TOPSIS. Initially the start speed of the vehicles is a slightly slower than the ideal. The

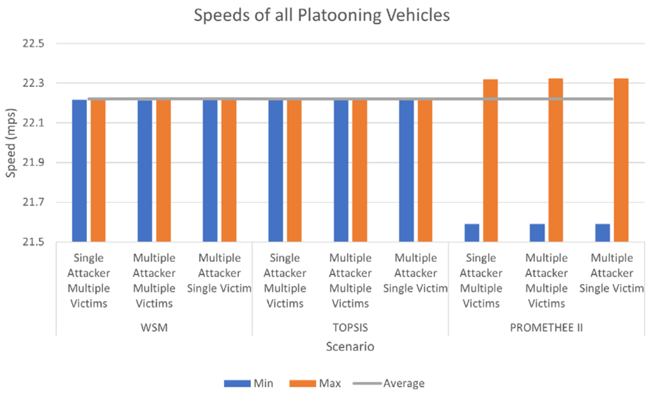


FIGURE 8 The average maximum, minimum speed and overall average vehicle speed.

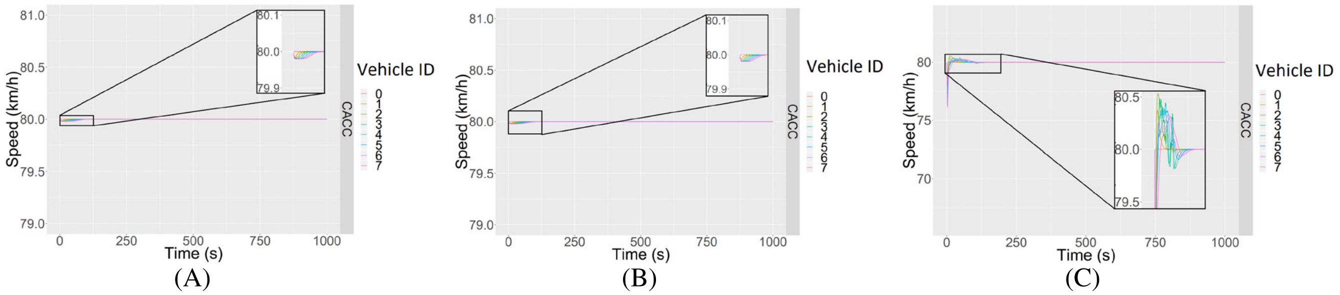


FIGURE 9 Single attacker, multiple victims: Speed of each vehicle when a single attacker attacks four members using (A) WSM, (B) TOPSIS, and (C) PROMETHEE II.

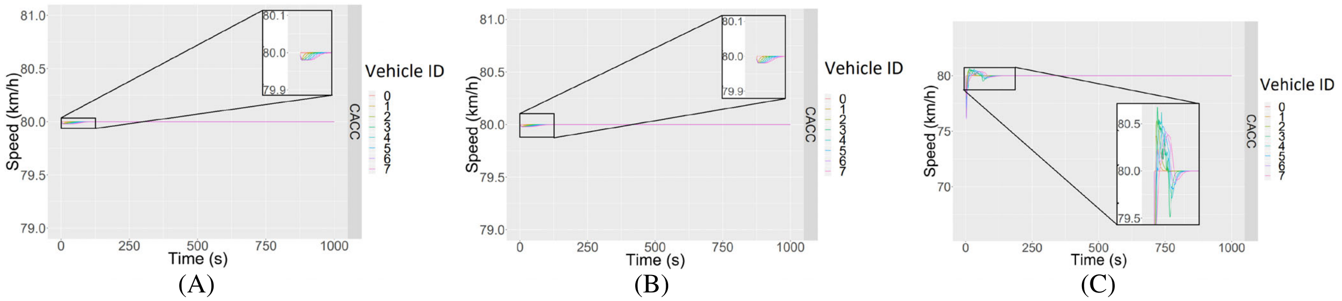


FIGURE 10 Multiple attackers, multiple victims: Speed of each vehicle when three attackers attack three platooning vehicles using (A) WSM (B) TOPSIS, and (C) PROMETHEE II.

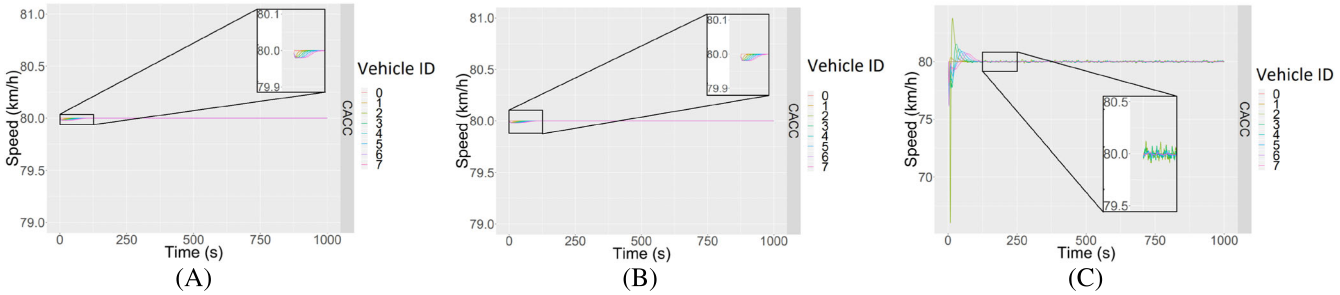


FIGURE 11 Multiple attackers, single victim: Speed of each vehicle when five attackers attack a single platooning vehicle using (A) WSM (B) TOPSIS, and (C) PROMETHEE II.

recovery is, however, smooth without any sudden changes in speed. This ideal behavior was expected due to the smooth and ideal inter-vehicle distance.

However, for PROMETHEE II results, the platoon is notably unstable when under FDI attack as depicted in Figures 9C–11C respectively. The method cannot hold the ideal vehicle speed for any vehicle after member vehicle one. The most disrupted vehicle is vehicle two, and the least is vehicle seven. Vehicle two sees its vehicle speed decrease to 65.89 kmph, which is a significant drop from the ideal speed of 80 kmph. Although brief, it is significantly destabilizing on the platoon with all following vehicles also needing to brake sharply to avoid collisions with the vehicle in front. After this period of braking, there an extended period of acceleration to 85.46 kmph on vehicle two before the speed returns to the ideal; however, unlike the WSM and TOPSIS vehicles, speed never returns to ideal when attacked by multiple attackers on a single member. While under attack by a single attacker or where there are multiple attackers attacking multiple members, the initial change in speed is small with the MCDM able to recover to the ideal. However when multiple attackers attack a single vehicle the disruption is significant and the member vehicles are unable to return to an ideal platooning speed.

WSM and TOPSIS methods again perform identically as they can prevent the FDI attacks from disrupting the platoon formation. Again the similarity in performance is because both methods are similar and will perform similarly. As for PROMETHEE II, it again struggled to maintain the ideal vehicle speed. In addition, PROMETHEE II cannot prevent the false beacons from being used by the CACC and rejecting some of the true beacons as fake, which is what causes PROMETHEE II to be unable to maintain the platoon formation.

5.3 | Environmental

A reduced CO_2 output of platooning vehicles is one of the major benefits of platooning and, as such, should be maintained under FDI attack. Figure 12 shows the average output of CO_2 for the platoons under each attacker model and each MCDM method. The WSM and TOPSIS platoon average CO_2 outputs of 3192.5 g per vehicle over the 1000 s of the simulation time or 3.193 g/s per vehicle. However, the PROMETHEE II CO_2 average outputs are slightly higher at between 3194 and 3194.5 g or 3.194–3.195 g/s per vehicle. This difference is very small; however over longer periods the total difference in CO_2 output will become significant.

Figure 13A–C show the average CO_2 output of each vehicle in the platoon with each attacker model applied. The WSM and TOPSIS again perform identically, with both able to keep all vehicles to the same CO_2 output. PROMETHEE II, however, only has vehicle one (the leader vehicle) outputting the same amount of CO_2 as seen in WSM and TOPSIS. All other vehicles output more CO_2. The most significant contributor is vehicle three during the attack scenario multiple attackers single victim. When multiple attackers are attacking a single vehicle, vehicle three sees the most significant CO_2 output as it is the directly attacked vehicle and as shown by Figures 7C and 11C. The vehicle cannot hold steady state

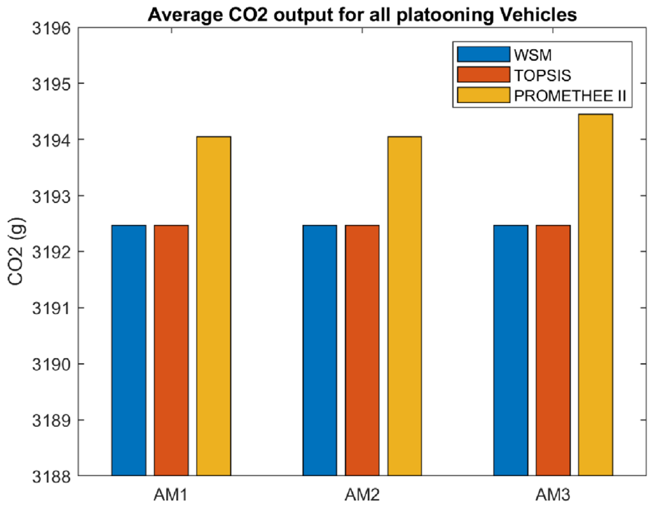
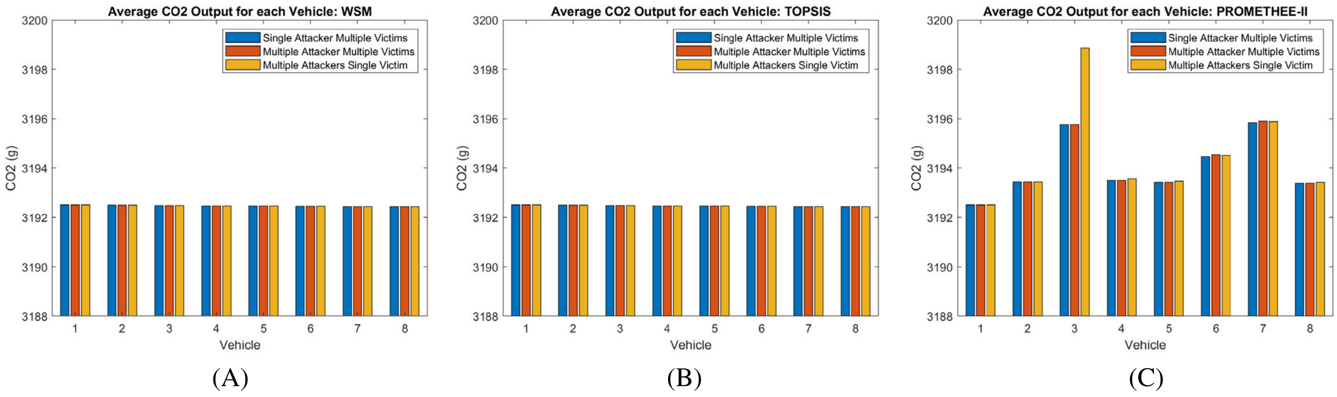


FIGURE 12 The average CO_2 output of each platoon.



(A) (B) (C)

FIGURE 13 The average CO_2 output of each vehicle in the platoon when using (A) WSM, (B) TOPSIS, and (C) PROMETHEE II.

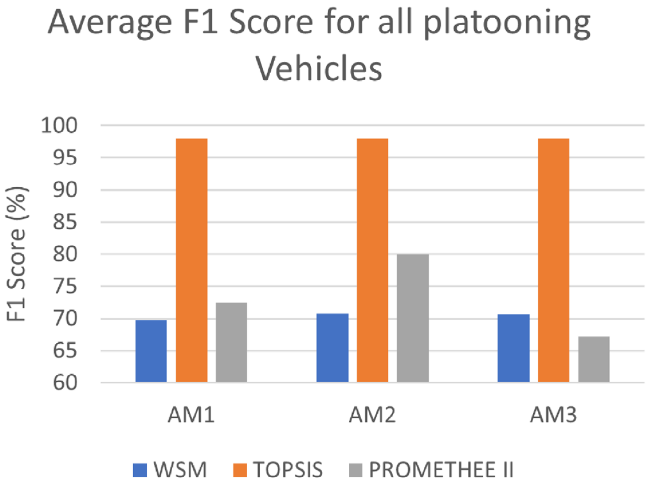


FIGURE 14 The average F1 score for each platoon.

platooning, which results in regular acceleration and breaking. This instability will cause the vehicle to consume more fuel, thus resulting in a higher CO_2 output.

WSM and TOPSIS both have very similar CO_2 outputs as the vehicle speed and inter-vehicle distance is the same. In the simulations performed, only vehicle speed and inter-vehicle distance affect the CO_2 output of the vehicle. PROMETHEE II, on the other hand, sees significant disruption to both inter-vehicle speed and vehicle speed, which is reflected in the amount of CO_2 produced by each platoon member. Vehicles that were, on average, more impacted by the attacks, like vehicle three (the first attack-able vehicle) and seven, saw significantly higher CO_2 outputs compared to other member vehicles.

5.4 | Cyber security

The F1 score is used in cyber security to represent the accuracy of the security method to prevent attacks.[44,45] Here the F1 score relates to how likely the MCDM will correctly identify a true beacon and send it to the CACC. The average F1 score of the platoon for each attacker model and MCDM method is shown in Figure 14. The F1 score is a percentage; therefore, the greater the score, the better the overall accuracy of the MCDM method at correctly identifying the true beacons from the false ones. First TOPSIS outperforms WSM and PROMETHEE II with an average score of 98% against all three attacker models. PROMETHEE II shows some promise here, able to outcompete WSM for the attack models single attacker multiple victims and multiple attackers multiple victims with an F1 score of 72% and 80% respectively,

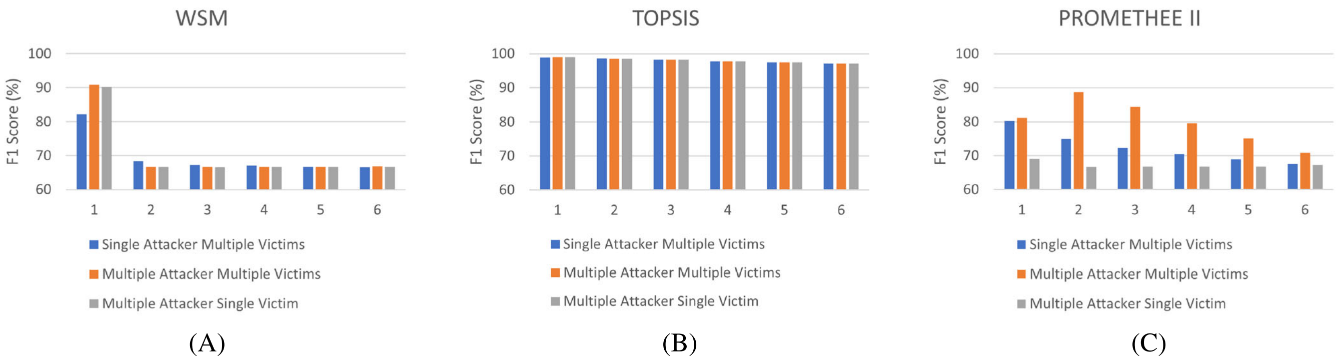


FIGURE 15 Average F1 score of each vehicle in the platoon when using (A) WSM, (B) TOPSIS, and (C) PROMETHEE II.

compared to WSM's 70% and 71%. Finally, for multiple attacker single victim, WSM obtains an F1 score of 71% compared to PROMETHEE II 69%.

Looking at the average F1 score for each vehicle that is vulnerable to attack from the attack models effectiveness of each MCDM method is shown in Figure 15A–C. TOPSIS is extremely capable here, with an F1 score ranging from 99% to 97% under all attack methods. On the other hand, PROMETHEE II is surprising as it can out-compete WSM on vehicle four, five, six, seven and eight. The WSM is very effective at 82% to 91% for the third vehicle; it performs poorly on all other vehicles. All other vehicles are unable to match this performance and so pull down the average F1 score for the whole platoon. PROMETHEE II, on the other hand, outperforms WSM for all other vehicles with F1 scores ranging from 89% to 67% whereas WSM sees its F1 score range between 68% and 66%. WSM and TOPSIS can maintain ideal performance regarding vehicle safety, stability and environmental impact, but when looking at the F1 score, WSM performs poorly. This means that while the WSM can maintain the platoon during the FDI attack, it is not very effective at correctly identifying beacons from member vehicles compared to the fake ones. With around a third of the beacons received by the WSM being mis-identified. With all other vehicles unable to match the first attacked vehicle's performance and, as such, pulling the average F1 score down for the whole platoon. While PROMETHEE II is less capable of maintaining safety and security compared to WSM, it is better overall at identifying real beacons in all members; however, it is less able to identify false beacons correctly, and this is why WSM outperforms it for safety and security.

6 | DISCUSSION

Results show that all three MCDM methods can maintain safe, stable, secure platoons with minimum environmental impact with varying degrees of success. TOPSIS outperforms the rest of the MCDM methods as it consistently performed well for all the aspects. WSM on the other hand match TOPSIS performance from safety, stability, and environmental aspect; however, it fails to accurately identify true beacons from false beacons, which is highlighted clearly by low F1 score. PROMETHEE II is a very different method of MCDM and, as such, performs differently overall. While it was better than WSM in terms of cyber security, the F1 scores are still very low overall. The PROMETHEE II method also performed poorly in safety and stability compared to WSM and TOPSIS as it was unable to maintain ideal platooning when under attack, with the inter-vehicle dropping to as low as 6 m, which put the vehicles at significant risk of collision.

For its robust and reliable performance under the attack models outlined in this article, it is TOPSIS that is the most promising method of MCDM to select beacons to be used in vehicle platooning to prevent FDI attacks. This conclusion is from the above-presented simulation work where the TOPSIS maintained a platoon of eight vehicles under various FDI attacks from between one and six attackers coordinating their attacks on the platoon. As a result, it was able to maintain ideal inter-vehicle distance and speed as well as keep down its CO_2 emissions. Not only that, but it was also extremely effective at correctly identifying the true beacon when under attack, which is important in a security method.

7 | CONCLUSION

Attacks on vehicle platoons are a real threat and potentially cause significant disruption. In this article, we proposed using MCDM, specifically WSM, TOPSIS, and PROMETHEE II, which can significantly reduce the impact of an attack on a platoon, by assessing the input beacon and comparing the beacon's information to past and predicted messages. Thus, by selecting the beacon that the platoon member calculates to be safe to use, MCDM can dampen the effects of the attacker on the platoon, as shown by the simulation results. Furthermore, this article shows that TOPSIS is the best at improving safety in a platoon by maintaining a consistent inter-vehicle distance and speed when under an attack; it is also able to maintain cyber security by identifying and removing all beacons not from a member vehicle.

In future, we will integrate MCDM with other intruder detection methods such as trust to ensure secure propagation of information in presence of attacker within the vehicular platoons.

CONFLICT OF INTEREST STATEMENT

All authors declare that they have no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Sean Joe Taylor https://orcid.org/0000-0001-7926-9800

REFERENCES

1. Willemsen D, Schmeitz A, Mascalchi E, et al. V2 platooning use cases, scenario definition and platooning levels. D2.3 of H2020 project ENSEMBLE; 2022. https://platooningensemble.eu/library/deliverables
2. Ellwanger S, Wohlfarth E. Truck platooning application. *IEEE Intelligent Vehicles Symposium (IV)*. IEEE; 2017:966-971.
3. Ma F, Yang Y, Wang J, et al. Eco-driving-based cooperative adaptive cruise control of connected vehicles platoon at signalized intersections. *Transp Res D Transp Environ*. 2021;92:102746. doi:10.1016/j.trd.2021.102746
4. Daems F. Platooning value and benefit analysis. D14.8 of H2020 project ENSEMBLE; 2022. www.platooningensemble.eu
5. Shi Y, Dhurjati P, Mascalchi E, Willemsen D. Preliminary safety case. D2.12 of H2020 project ENSEMBLE; 2022. www.platooningensemble.eu
6. Petrillo A, Pescapé A, Santini S. A collaborative approach for improving the security of vehicular scenarios: the case of platooning. *Comput Commun*. 2018;122:59-75. doi:10.1016/j.comcom.2018.03.014
7. Santhosh J, Sankaran S. Defending against sybil attacks in vehicular platoons. *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE; 2019:1-6.
8. Boeira F, Barcellos MP, de Freitas EP, Vinel A, Asplund M. On the impact of sybil attacks in cooperative driving scenarios. *IFIP Networking Conference (IFIP Networking) and Workshops*. IEEE; 2017:1-2.
9. Amoozadeh M, Raghuramu A, Chuah C-N, et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun Mag*. 2015;53(6):126-132. doi:10.1109/MCOM.2015.7120028
10. Taylor SJ, Ahmad F, Nguyen HN, Shaikh SA, Evans D, Price D. Vehicular platoon communication: cybersecurity threats and open challenges. *51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE; 2021:19-26.
11. van der Heijden R, Lukaseder T, Kargl F. Analyzing attacks on cooperative adaptive cruise control (CACC). *IEEE Vehicular Networking Conference (VNC)*. IEEE; 2017:45-52.
12. Amoozadeh M, Deng H, Chuah C-N, Zhang HM, Ghosal D. Platoon management with cooperative adaptive cruise control enabled by VANET. *Veh Commun*. 2015;2(2):110-123. doi:10.1016/j.vehcom.2015.03.004
13. Al-kahtani MS. Survey on security attacks in vehicular ad hoc networks (VANETs). *6th International Conference on Signal Processing and Communication Systems*. IEEE; 2012:1-9.
14. Zhang D, Shen Y-P, Zhou S-Q, Dong X-W, Yu L. Distributed secure platoon control of connected vehicles subject to DoS attack: theory and application. *IEEE Trans Syst Man Cybern Syst*. 2021;51(11):7269-7278. doi:10.1109/TSMC.2020.2968606
15. Taylor SJ, Ahmad F, Nguyen HN, Shaikh SA, Evans D. Safety, stability and environmental impact of FDI attacks on vehicular platoons. *IEEE/IFIP Network Operations and Management Symposium (NOMS)*. IEEE; 2022:1-6.
16. Wolf M, Willecke A, Müller J-C, et al. Securing CACC: strategies for mitigating data injection attacks. *IEEE Vehicular Networking Conference (VNC)*. IEEE; 2020:1-7.
17. Lai C, Lu R, Zheng D. SPGS: a secure and privacy-preserving group setup framework for platoon-based vehicular cyber-physical systems. *Secur Commun Netw*. 2016;9(16):3854-3867. doi:10.1002/sec.1523
18. Li K, Lu L, Ni W, Tovar E, Guizani M. Secret key agreement for data dissemination in vehicular platoons. *IEEE Trans Veh Technol*. 2019;68(9):9060-9073. doi:10.1109/TVT.2019.2926313
19. Bermad N, Zemmoudj S, Omar M. Securing vehicular platooning against vehicle platooning disruption (VPD) attacks. *8th International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*. IEEE; 2019:1-6.
20. Ucar S, Ergen SC, Ozkasap O. IEEE 802.11p and visible light hybrid communication based secure autonomous platoon. *IEEE Trans Veh Technol*. 2018;67(9):8667-8681. doi:10.1109/TVT.2018.2840846

21. Ji Y, Hou R, Lui K-S, Li H. A blockchain-based vehicle platoon leader updating scheme. *2020 IEEE International Conference on Communications (ICC)*. IEEE; 2020:1-6.
22. Junaidi DR, Ma M, Su R. Effective authentication to prevent sybil attacks in vehicular platoons. *2022 17th International Conference on Control, Automation, Robotics and Vision (ICARCV)*. IEEE; 2022:949-954.
23. Kylili A, Christoforou E, Fokaides PA, Polycarpou P. Multicriteria analysis for the selection of the most appropriate energy crops: the case of cyprus. *Int J Sustain Energy*. 2016;35(1):47-58. doi:10.1080/14786451.2014.898640
24. Mardani A, Jusoh A, Zavadskas EK, Cavallaro F, Khalifah Z. Sustainable and renewable energy: an overview of the application of multiple criteria decision making techniques and approaches. *Sustainability*. 2015;7(10):13947-13984. doi:10.3390/su71013947
25. Elgaroui L, Pierre S, Chamberland S. New routing protocol for reliability to intelligent transportation communication. *IEEE Trans Mob Comput*. 2021;22:2281-2294. doi:10.1109/TMC.2021.3116157
26. Arif M, Kumar VD, Jayakumar L, Ungurean I, Izdrui D, Geman O. DAHP-TOPSIS-based channel decision model for co-operative CR-enabled Internet on Vehicle (CR-IoV). *Sustainability*. 2021;13(24):13966. doi:10.3390/su132413966
27. Sharma S, Kaul A. Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET. *Veh Commun*. 2018;12:23-38. doi:10.1016/j.vehcom.2017.12.003
28. Nandy T, Idris MYIB, Noor RM, Ahmedy I, Bhattacharyya S. A multiple-criteria decision analysis clustering and cluster head selection algorithm in vehicular network. *IEEE 8th R10 Humanitarian Technology Conference (R10-HTC)*. IEEE; 2020:1-6.
29. Burkacky O, Deichmann J, Klein B, Pototzky K, Scherf G. Cybersecurity in automotive. Technical Repport, McKinsey; March 2020.
30. Harkness V, Clark J, Perry R, et al. Future threats to ITS networks and CAV infrastructure; 2020. Accessed September 13, 2022. https://www.f-secure.com/content/dam/f-secure/en/consulting/our-thinking/collaterals/digital/consulting-future-threats-cav-report.pdf
31. Bikmukhamedov R, Yeryomin Y, Seitz J. Evaluation of MCDA-based handover algorithms for mobile networks. *Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE; 2016:810-815.
32. Chettibi S. Combination of HF set and MCDM for stable clustering in VANETs. *IET Intell Transp Syst*. 2020;14(3):190-195. doi:10.1049/iet-its.2019.0283
33. Pezzano A, Dhurjati P, Mascalchi E, et al. Final version hazard analysis and risk assessment and functional safety concept. D2.14 of H2020 project ENSEMBLE; 2022. www.platooningensemble.eu
34. Rathee G, Ahmad F, Iqbal R, Mukherjee M. Cognitive automation for smart decision-making in industrial Internet of things. *IEEE Trans Industr Inform*. 2021;17(3):2152-2159. doi:10.1109/TII.2020.3013618
35. Ganin AA, Quach P, Panwar M, et al. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Anal*. 2020;40(1):183-199.
36. Rezaei J. Best-worst multi-criteria decision-making method. *Omega*. 2015;53:49-57. doi:10.1016/j.omega.2014.11.009
37. Garlichs K, Willecke A, Wegner M, Wolf LC. TriP: misbehavior detection for dynamic platoons using trust. *IEEE Intelligent Transportation Systems Conference (ITSC)*. IEEE; 2019:455-460.
38. Hwang C-L, Yoon K. *Methods for Multiple Attribute Decision Making*. Springer; 1981:58-191.
39. Segata M, Joerer S, Bloessl B, Sommer C, Dressler F, Cigno RL. Plexe: a platooning extension for Veins. *2014 IEEE Vehicular Networking Conference (VNC)*. IEEE; 2014:53-60.
40. Sommer C, German R, Dressler F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Trans Mob Comput*. 2011;10(1):3-15. doi:10.1109/TMC.2010.133
41. OMNET. OMNeT++: discrete event simulator. Accessed September 13, 2022. https://omnetpp.org/
42. SUMO. Simulation of urban MObility. Accessed September 9, 2022. https://www.eclipse.org/sumo/
43. Shladover S, Lu X-Y, Yang S, et al. Cooperative adaptive cruise control (CACC) for partially automated truck platooning: final report. Escholarshiporg; 2018. https://escholarship.org/uc/item/260060w4#main
44. Chen Y-M, Wei Y-C. A beacon-based trust management system for enhancing user centric location privacy in VANETs. *J Commun Netw*. 2013;15(2):153-163. doi:10.1109/JCN.2013.000028
45. Ahmad F, Kurugollu F, Kerrache CA, Sezer S, Liu L. NOTRINO: a NOvel hybrid TRust management scheme for INternet-of-vehicles. *IEEE Trans Veh Technol*. 2021;70(9):9244-9257. doi:10.1109/TVT.2021.3049189

How to cite this article: Taylor SJ, Ahmad F, Nguyen HN, Shaikh SA, Bryans J, Wartnaby CE. A comparative analysis of multi-criteria decision methods for secure beacon selection in vehicular platoons. *Trans Emerging Tel Tech*. 2023;e4841. doi: 10.1002/ett.4841