CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

A Smart Energy-based Source Location Privacy Preservation (SESLPP) Model for IoT-based VANETs

Special Issue Article

Abizar Khalil
Haleem Farman
Bilal Jan
Zahid Khan
Anis Koubâa*

*CISTER Research Centre

CISTER-TR-200307

2020

A Smart Energy-based Source Location Privacy Preservation (SESLPP) Model for IoT-based VANETs

Abizar Khalil, Haleem Farman, Bilal Jan, Zahid Khan, Anis Koubâa*

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: aska@isep.ipp.pt

https://www.cister-labs.pt

Abstract

Vehicle-to-Vehicle (V2V) communication aims to improve road safety by periodic exchange of Hello messages. Nowadays, the Internet of Things (IoT) is widely used to solve city transportation problems by employing multihop-based V2V communication. In IoT-based vehicular ad-hoc networks (VANETs), devices are interconnected with various hardware and software, so the privacy of data, temporal, and location will be at risk due to unauthorized manipulation, especially at intersections in congested urban areas. To address these concerns in IoT-based VANETs, we proposed a Smart Energy-based Source Location Privacy Preservation (SESLPP) technique for sustainable urban city roads (i.e., Intersections). The proposed SESLPP protects the source location privacy while maintaining an accurate reputation based on specific parameters such as trust, speed, distance, and acceleration. A selected node based on these parameters forwards messages and acts as a phantom node to improve the source location privacy within their communication range. The selection of a phantom node is based on a set of parameters, which makes it a multi-criteria decision problem. In this paper, a multi-criteria decision tool known as Analytical Network Process (ANP) has been used for optimal phantom node selection that improves the source location privacy in an urban scenario by considering intersections. We considered the same parameters (trust, speed, distance, and acceleration) that was used for highway scenario with proper adjustment of their values for an urban area (cross-road intersection point). The proposed SESLPP provides an optimal platform for smart city communication networks.

Received: 27 November 2019 | Revised: 7 February 2020 | Accepted: 10 March 2020

DOI: 10.1002/ett.3973

SPECIAL ISSUE ARTICLE

WILEY

A smart energy-based source location privacy preservation model for Internet of Things-based vehicular ad hoc networks

Abizar[1] | **Haleem Farman**[1] | **Bilal Jan**[2] | **Zahid Khan**[3] | **Anis Koubaa**[3]

[1]Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan

[2]Department of Computer Science, FATA University, Kohat, Pakistan

[3]Robotics and Internet-of-Things Lab, Prince Sultan University, Riyadh, Saudi Arabia

Correspondence
Zahid Khan, Robotics and Internet-of-Things Lab, Prince Sultan University, Riyadh, Saudi Arabia.
Email:zskhan@psu.edu.sa

Abstract

Vehicle-to-vehicle (V2V) communication aims to improve road safety by periodic exchange of Hello messages. Nowadays, the Internet of Things (IoT) is widely used to solve city transportation problems by employing multihop-based V2V communication. In IoT-based vehicular ad hoc networks (VANETs), devices are interconnected with various hardware and software, so the privacy of data, temporal, and location will be at risk due to unauthorized manipulation, especially at intersections in congested urban areas. To address these concerns in IoT-based VANETs, we proposed a smart energy-based source location privacy preservation (SESLPP) technique for sustainable urban city roads (ie, intersections). The proposed SESLPP protects the source location privacy while maintaining an accurate reputation based on specific parameters such as trust, speed, distance, and acceleration. A selected node based on these parameters forwards messages and acts as a phantom node to improve the source location privacy within their communication range. The selection of a phantom node is based on a set of parameters, which makes it a multicriteria decision problem. In this article, a multicriteria decision tool known as analytical network process has been used for optimal phantom node selection that improves the source location privacy in an urban scenario by considering intersections. We considered the same parameters (trust, speed, distance, and acceleration) that was used for highway scenario with proper adjustment of their values for an urban area (crossroad intersection point). The proposed SESLPP provides an optimal platform for smart city communication networks.

1 | INTRODUCTION

In Internet of Things (IoT)-based vehicular ad hoc networks (VANETs), vehicles act as nodes that communicate with each other directly or through road side units (RSUs). In addition, VANETs play a vital role in providing a high level of safety to drivers on the road,[1,2] such as accident information,[3] traffic monitoring,[4] and information regarding road conditions, and so on.[5] IoT-based VANETs operate in different communication modes, that is, vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), and vehicle-to-everything (V2X).[6,7] Nowadays, VANET is used as tool by the intelligent transportation systems (ITS)[8] to solve different transportation issues such as traffic congestion detection and avoidance.

Day by day the number of vehicles on road increases due to the increase in population and the lifestyle of people who use vehicles on daily basis for their routine activities. Mostly people want to get the benefits of VANETs but do not want to share their location information to preserve privacy. In this era of connected devices, it becomes very challenging to preserve location in densely connected network. False messages can be disseminated in the network, which can misguide people. Due to wireless connectivity, VANETs are more vulnerable to security attacks. Any vehicle with a suitable receiver can analyze and interrupt communications in IoT-based VANETs. The attacker can interact with vehicles in the network by using radio transceivers. It is possible for adversaries to find the source location even if strong data encryption methods are used. It is important to preserve the location privacy and not to expose information regarding network traffic in quick time by not wasting much resources. It is very hard to completely eliminate the issues of location privacy; however, the contents of a message can be assured using encryption methods. The industry and academia are trying to improve security and privacy issues in IoT-based VANETs.

In literature, various models have been proposed to strengthen the location privacy of vehicles in VANETs. In Reference 9, an efficient conditional privacy preservation (ECPP) is proposed that uses RSUs and OBUs to disseminate safety messages with registration authority by using anonymous authentication. This results in maintaining a large number of key pairs that need to be stored at each OBU. Moreover, another problem is that if some OBUs cancel anonymous keys, then every OBU updates the list that consumes long time. Onion-based anonymous routing protocol is proposed based on source, destination, and route anonymity feature. Vehicles are dynamically grouped to form onion relays.[10] One of the feature of this method is that the onion chain can be modified to maintain location privacy and for better performance, it can be cut down to small chain. Digital signatures are used in Reference 11 for authentication using public key. However, in urban areas where the number of vehicles are in large number will have delay in verification of messages. Moreover, it has no more trusted certificate cancellation in a long certificate revocation list.

The aforementioned schemes have enhanced the location privacy of the source nodes in IoT-based VANETs; still, there is possibility of improvement by choosing a trusted node for privacy preservation. Farman et al[12] also proposed a multicriteria-based location privacy preservation model for highway vehicular scenarios. The authors in Reference 12 ignored the location privacy in urban scenarios (ie, highly congested intersection points). Normally, on intersection points, vehicles are not frequently in mobility due to massive congestion in peak hours compared with highway roads. Thus, the junction points will be highly vulnerable to privacy issues. To cope with this persistent challenge, it is necessary to extend the multicriteria-based privacy to urban city networks. Second, in Reference 12, the values of the parameters were set according to the highway mobility constraints. Here, in this article, we used different values in order to set the reference[12] model to urban city scenario. In summary, this work extends the work in Reference 12 by considering urban scenarios with highly congestion road intersections.

To improve the location privacy of communicating vehicles, we proposed a smart energy-based source location privacy preservation (SESLPP) model using analytical network process (ANP) for road intersection points in urban cities. SESLPP aims to select an optimal phantom node based on certain parameters such as trust, speed, distance, and acceleration. The ANP is used as a multicriteria decision tool to select the most suitable trusted phantom node. The ANP was introduced to solve the interdependencies in intercluster or intraclusters. ANP is appropriate in certain cases where parameters have influence on each other and require feedback as well. Here, in our model, ANP is used to select an optimum node as a trusted phantom node to process the dependencies of elements to bring the essential outcome. Furthermore, the criteria ranking and other elements are considered for decision making. Each time a source node is changed, a new phantom node is selected so that to make it hard for the attackers to track the position of the source node.

The remaining parts are structured as follow: Section 2 illustrates the proposed technique and describes the phantom node selection using ANP. Results and discussions are analyzed in Section 3, while finally, the article is concluded in Section 4.

2 | SESLPP MODEL

In this article, we have proposed a technique for the source location privacy in IoT-based VANETs. The proposed technique considers V2V communication in which vehicles communicate with each other. A trust-based source location privacy preservation model for IoT-based VANETs is proposed that protects source location while maintaining an accurate reputation. Moreover, the decision of selection is depended on particular factors such as trust, speed, distance, and acceleration, as shown in Table 1.

TABLE 1 Parameters description

Parameters	Variable
Trust	Tr
Acceleration	Ac
Speed	Sp
Distance	Dist

The selected node forwards messages and acts as a phantom node to enhance the source location privacy inside its communication coverage. To understand the proposed solution, it is also important to understand the trust models.

2.1 | Trust model

For a vehicle to satisfy the criteria of a phantom node, it requires some constraints to fulfill, including trust. Therefore, it is difficult for an adversary node to be selected as a phantom node in the proposed model. The trust model has three subtypes as follows.

1. *Entity-oriented trust model:* In this model, only trusted vehicles disseminate information, which is called trusted messages. The entity-oriented trust model is based on vehicles' role and supported experiences/observation. Furthermore, the vehicles' roles are considered authoritative, official, and ordinary.[13]
2. *Data-oriented trust models:* Different from entity-orientated fashions, whether the message could be common with the aid of a receiver is depended on the message itself rather than the message sender, for example, piggybacking. A vehicle publishes a message reporting a certain occurrence. Most vehicles receive the message and most receivers then transmit them in compliance with a certain policy. Each forwarder has a separate opinion. This opinion is based on one's observations and previous views that are added to it by previous transmitters, and one important benefit of this approach is that the opinions of various vehicles have different weights.[14]
3. *Combined trust model:* Three hybrid trust models are suggested to measure peer trustworthiness and use modeling outcomes to determine data reliability. Developing a distributed model of credibility using a notion called piggyback of opinion where each forwarding peer (of an event message) contributes its view to the trust of the data. The suggested models are based on an algorithm that allows the peers to generate an opinion about the data based on collated views. The opinion and various other trust indicators including direct trust, indirect trust, sender-based reputation level, and geo-situation-oriented reputation level are attached to the message.[15]

2.2 | System model

It is assumed that the source node communicates through the trusted phantom node in an urban city road scenario (congested intersection point), as shown in Figure 1. Each time the source chooses different phantom node for communication to make it hard for attackers to track the position of the source node.

Here, a multicriteria decision tool, that is, ANP, is used for the optimal phantom node selection. The ANP is used for decision making and selection of suitable choice. In the proposed urban scenario, as shown in Figure 1, it is considered that when a vehicle wants to communicate with other vehicles, then it becomes a source node and sends packets to a phantom node based on trust, distance, acceleration, and speed of that particular vehicle. Phantom nodes are considered as trusted vehicles and therefore divided into categories based on the parameters mentioned in Table 1. Trust[16] shows the priority of a node on another in the network. It is based on the hope that the other node will perform a specific action believed/predicted/accepted by an originator. Distance[17,18] is measured in meters between the sender and receiver, while speed[17] can be expressed as the rate of displacement of a particular vehicle in the network. The acceleration is defined as the variation in vehicle's velocity with respect to time.[17,19]

The source node also ranks the nodes in communication range with their respective values. For example, if a phantom node leaves the network, then the next node on the list is selected as a phantom node. The source location must be protected from an adversary. The network may be dense. Thus, nodes (vehicles) authenticate trusted nodes after coming

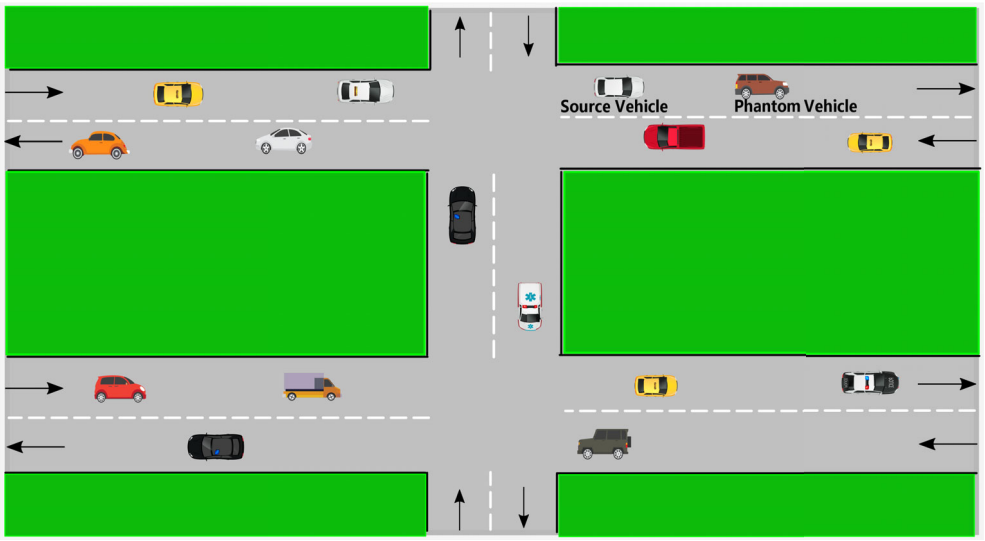

FIGURE 1 Proposed urban scenario

close together. It is assumed that the level of trust ranges from 1 to 9,[20] that is, low to high. The maximum speed considered is 90 km/h, and the minimum is 1 to 20 km/h. The distance between nodes is 5 to 10 m graded 1 to 9 ratio. The acceleration of a node is 90 m/s^2 maximum, for example, 10 m/s^2 acceleration is graded as 1. For instance, if the first communication is made through node A, then next time the first vehicle (source) might communicate through trusted node B or C. Therefore, the phantom node is different after each communication to protect the location of the source. Similarly, if the receiving node wants to forward this message to other nodes, another phantom node (node B or C) is selected, and the message is forwarded through that phantom node. The process continues until the message reaches the last node in the network.

2.3 | Phantom node selection using ANP

In the proposed technique, multiple parameters are used for the selection of phantom node that makes it a multicriteria decision making (MCDM) problem. The MCDM has a number of complex decision-making applications. As mentioned earlier, a multicriteria decision tool (ie, ANP) is used for the selection of phantom node at intersections where usually congestion rate is high. In ANP, the network is structured into goal, criteria, and alternatives. The ANP tool has been used in many applications for complex decision making.[21-24] The first step is to decompose the problem into subproblems, whereas goals, alternatives, and criteria are identified, as shown in Figure 2.

2.3.1 | Pairwise comparison of elements and criteria

A very important step is to compare each element of criteria with each element of alternative and vice versa. The elements in ith row are compared with jth column's elements. If the value of ith row is higher than jth column, then it is written as (ij), where (ji) represents its reciprocal value. Elements are pairwise compared according to the 9-point quantitative scale presented by Saaty,[25] as shown in Table 2. The scale is converted into a quantitative scale of the range between 1 and 9. The comprehensive importance is computed by calculating the principal of eigenvalue and associated eigenvector of the comparison matrix. After calculating these values, the consistency index is measured. The priority of vector w is calculated in Equation (1).

$$Aw = \lambda_{\max} * w. \tag{1}$$

Here $\lambda_{\max}$ is the highest eigenvalue of matrix "A," while "w" is the eigenvector. The value of λ is obtained by adding column of the matrix, times the normalized eigenvector. The most important eigenvector is obtained by the addition of all λ.

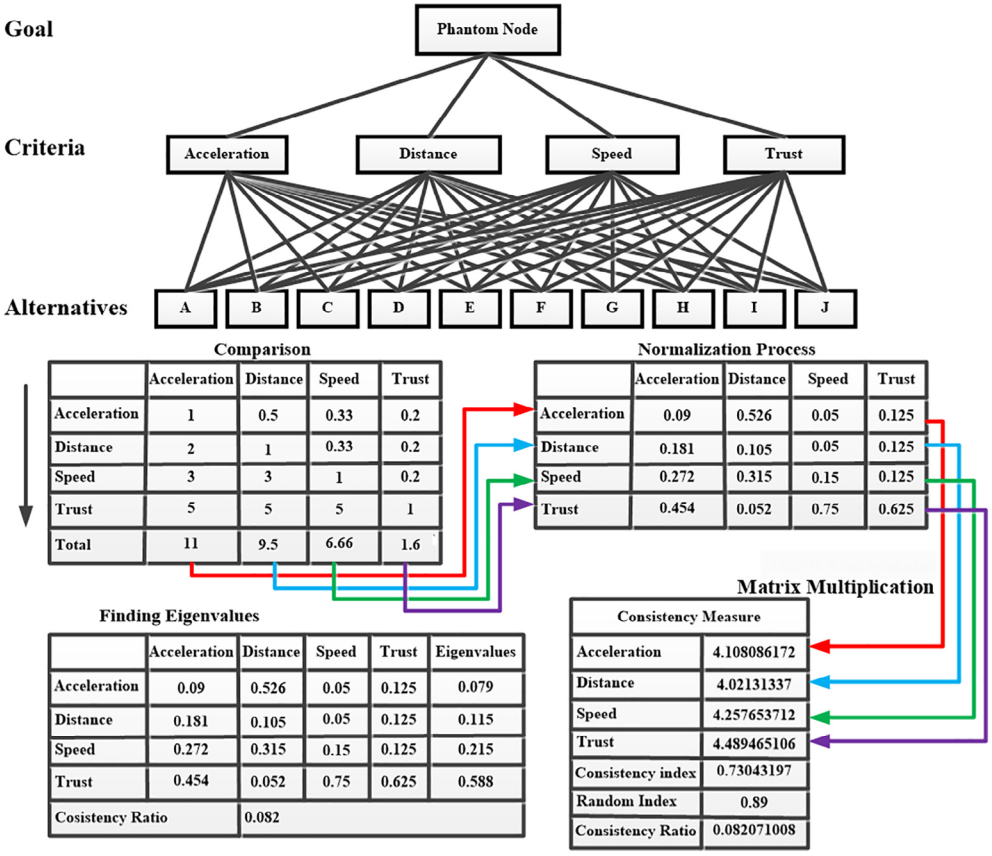

FIGURE 2 Graphical illustration of analytical network process method

Comparison	Acceleration	Distance	Speed	Trust
Acceleration	1	0.5	0.33	0.2
Distance	2	1	0.33	0.2
Speed	3	3	1	0.2
Trust	5	5	5	1
Total	11	9.5	6.66	1.6

Normalization Process	Acceleration	Distance	Speed	Trust
Acceleration	0.09	0.526	0.05	0.125
Distance	0.181	0.105	0.05	0.125
Speed	0.272	0.315	0.15	0.125
Trust	0.454	0.052	0.75	0.625

Finding Eigenvalues	Acceleration	Distance	Speed	Trust	Eigenvalues
Acceleration	0.09	0.526	0.05	0.125	0.079
Distance	0.181	0.105	0.05	0.125	0.115
Speed	0.272	0.315	0.15	0.125	0.215
Trust	0.454	0.052	0.75	0.625	0.588
Cosistency Ratio	0.082				

TABLE 2 The fundamental scale of absolute numbers

Particulars	Level	Explanation
Equal importance	1	Two actions contribute in the same way to the objective
Weak or slight	2	
Moderate importance	3	Experience and judgment to some extent favor one movement over another
Moderate plus	4	
Strong importance	5	Experience and judgment powerfully favor one activity over another
Strong plus	6	
Very strong	7	An activity is favored very powerfully over another
Very, very strong	8	
Extremely Important	9	The evidence favoring one activity over another is of the highest possible order of confirming.

The consistency index (CI) and consistency ratio (CR) of pairwise comparison matrix are calculated through Equations (2) and (3).[20]

$$\mathrm{CI} = \frac{(\lambda_{\max} - n)}{n - 1}, \tag{2}$$

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}}. \tag{3}$$

The random consistency index (RI) is given by Reference 25, as shown in Table 3. The value of CR must be less than 0.1. If it exceeds 0.1, then revise the comparison. A supermatrix is gained by merging all comparison matrices. In

TABLE 3 Random consistency index

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
R1	0	0	0.52	0.89	1.11	1.25	1.35	1.4	1.45	1.49	1.52	1.54	1.56	1.58	1.59

TABLE 4 Parameters and their assigned weights

Node	Trust	Speed	Distance	Acceleration
A	8	5	3	2
B	5	8	7	5
C	6	6	5	3
D	4	7	4	3
E	5	5	6	4
F	7	6	4	3
G	3	5	8	9
H	2	9	7	6
I	9	4	2	1
J	6	4	3	6

TABLE 5 $N \times N$ pairwise comparisons

	Ac	Dist	Sp	Tr
Ac	1			
Dist		1		
Sp			1	
Tr				1

supermatrix, if the column sum is greater than 1, then it will be normalized till column values become equivalent to or less than 1. Transform the weighted supermatrix (concise matrix column sum is less than or equal to 0.1) to the limit matrix. Pick the most suitable alternative from the limit matrix table. Mathematically, the selection of optimal node is represented as:[26]

$$\text{selection} = \sum_{p \in i} Pi, \tag{4}$$

where P is the acceleration, distance, speed, and trust. According to the ANP algorithm,[25] the ultimate scales for judgment are given in Table 2, which shows the relative importance of each component. All values have been graded in terms of trust, speed, distance, and acceleration from 1 to 9 ratio. The nodes have been compared and graded both parameterwise as well as nodewise. The parameters and their values are presented in Table 4.

Once the parameter weights are decided, the step-by-step ANP process for phantom node selection is followed. The proposed model has used values given in Table 5 into a $n \times n$ matrix for a pairwise comparison. Relative weights of components (parameters and nodes) are shown as C_{ij}, where "i" represents row and "j" is used for column. If the relative importance of component C^i is equal to component C_j then $C_{ij} = 1, C_{ji} = 1$, as presented in Table 5. The weight at diagonal is 1, which represents the same importance.

Table 7 represents the normalization process involved in the pairwise comparison as shown in Tables 5 and 6. Table 8 shows the eigenvalues obtained from Table 7.

To find eigenvalues (Table 8), the sum of columns (Table 6) and sum of rows (Table 7) are multiplied. The next step is to calculate the consistency ratio using the formula in Equation (3), as shown in Figure 2. The same process is followed for the remaining matrices from Tables 9 to 21.

TABLE 6 Comparison of node A with respect to acceleration

	Ac	Dist	Sp	Tr
Ac	1	0.5	0.33	0.2
Dist	2	1	0.33	0.2
Sp	3	3	1	0.2
Tr	5	5	5	1
Total	11	9.5	6.66	1.6

TABLE 7 Normalization process

Ac	0.09	0.526	0.05	0.125
Dist	0.181	0.105	0.05	0.125
Sp	0.272	0.315	0.15	0.125
Tr	0.454	0.052	0.75	0.625

TABLE 8 Finding the eigenvalues

	Ac	Dist	Sp	Tr	EV
Ac	0.09	0.0526	0.05	0.125	0.079
Dist	0.1818	0.105	0.05	0.125	0.115
Sp	0.272	0.315	0.15	0.125	0.215
Tr	0.4545	0.052	0.75	0.625	0.588
CR	0.082				

TABLE 9 Pairwise comparison of parameters with respect to node B

	Ac	Dist	Sp	Tr	EV
Ac	1	0.05	0.33	0.2	0.081
Dist	2	1	2	0.2	0.172
Sp	0.3333	0.5	1	0.2	0.147
Tr	0.5	5	5	1	0.598
CR	0.082				

TABLE 10 Pairwise comparison of parameters with respect to node C

	Ac	Dist	Sp	Tr	EV
Ac	1	0.05	0.33	0.2	0.081
Dist	2	1	2	0.2	0.172
Sp	3	0.5	1	0.2	0.147
Tr	5	5	5	1	0.598
CR	0.08				

TABLE 11 Pairwise comparison of parameters with respect to node D

	Ac	Dist	Sp	Tr	EV
Ac	1	0.05	0.5	0.2	0.089
Dist	2	1	1	0.2	0.147
Sp	2	1	1	0.2	0.147
Tr	5	5	5	1	0.614
CR = 0.02					

	Ac	Dist	Sp	Tr	EV
Ac	1	0.33	0.33	0.20	0.075
Dist	3	1	2	0.25	0.210
Sp	3	0.5	1	0.25	0.154
Tr	5	4	4	1	0.559
CR = 0.05					

TABLE 12 Pairwise comparison of parameters with respect to node E

	Ac	Dist	Sp	Tr	EV
Ac	1	0.333	0.5	0.2	0.080
Dist	3	1	3	0.2	0.224
Sp	2	0.333	1	0.25	0.125
Tr	5	5	4	1	0.570
CR = 0.08					

TABLE 13 Pairwise comparison of parameters with respect to node F

	Ac	Dist	Sp	Tr	EV
Ac	1	0.5	0.5	0.2	0.089
Dist	2	1	3	0.25	0.209
Sp	2	0.333	1	0.2	0.120
Tr	5	4	5	1	0.579
CR = 0.06					

TABLE 14 Pairwise comparison of parameters with respect to node G

	Ac	Dist	Sp	Tr	EV
Ac	1	0.5	0.5	0.2	0.094
Dist	2	1	0.333	0.333	0.145
Sp	2	3	1	0.333	0.246
Trust	5	3	3	1	0.514
CR = 0.06					

TABLE 15 Pairwise comparison of parameters with respect to node H

	Ac	Dist	Sp	Tr	EV
Ac	1	0.5	0.333	0.2	0.083
Dist	2	1	0.333	0.25	0.127
Sp	3	3	1	0.333	0.256
Tr	5	4	3	1	0.532
CR = 0.040					

TABLE 16 Pairwise comparison of parameters with respect to node I

TABLE 17 Pairwise comparison of parameters with respect to node J

	Ac	Dist	Sp	Tr	EV
Ac	1	0.33	0.5	0.16	0.072
Dist	3	1	3	0.2	0.21
Sp	2	0.33	1	0.16	0.105
Tr	5.99	5	5.99	1	0.618
CR= 0.063					

TABLE 18 Pairwise comparison with respect to acceleration

	A	B	C	D	E	F	G	H	I	J
A	1	0.333	1	1	0.5	1	0.142	0.25	1	0.25
B	3	1	2	2	1	2	0.25	1	4	1
C	1	0.5	1	1	1	1	0.166	0.333	2	0.333
D	1	0.5	1	1	1	1	0.166	0.333	2	0.333
E	2	1	1	1	1	1	0.2	0.5	3	0.5
F	1	0.5	1	1	1	1	0.166	0.333	2	0.333
G	7	4	5.999	5.999	5	5.999	1	0.333	8	3
H	4	1	3	3	2	3	0.333	1	5	1
I	1	0.25	0.5	0.5	0.3333	0.5	0.125	0.2	1	0.2
J	4	1	3	3	2	3	0.333	1	5	1

TABLE 19 Pairwise comparison of nodes with respect to distance

	A	B	C	D	E	F	G	H	I	J
A	1	0.25	0.5	1	0.5	1	0.2	0.25	1	1
B	4	1	2	3	1	3	1	1	5	4
C	2	0.5	1	1	1	1	0.33	0.5	3	2
D	1	0.33	1	1	1	1	0.25	0.33	2	1
E	3	1	1	2	1	2	0.5	1	4	3
F	1	0.33	1	1	1	1	0.25	0.33	2	1
G	5	1	3	4	5	4	1	1	5.99	5
H	4	1	2	3	2	3	1	1	5	4
I	1	0.2	0.33	0.5	0.33	0.5	0.166	0.2	1	1
J	1	0.25	0.5	1	2	1	0.2	0.25	1	1

The following values from Tables 18 to 21 are used for node comparisons with respect to parameters.

2.3.2 | Unweighted supermatrix

The pairwise comparisons are constructed through Saaty's quantitative scale that is from 1 to 9, where 1 represents the equivalent position and 9 is the highest weight of one element over another. The local weights obtained through comparison matrix are represented in unweighted supermatrix, as presented in Table 22.

TABLE 20 Pairwise comparison of nodes with respect to speed

	A	B	C	D	E	F	G	H	I	J
A	1	0.33	1	0.5	1	1	1	0.25	1	1
B	3	1	2	1	3	2	3	1	4	4
C	1	0.5	1	1	1	1	1	0.33	2	2
D	2	1	1	1	2	1	2	0.5	3	3
E	1	0.33	1	0.5	1	1	1	0.25	1	1
F	1	0.5	1	1	1	1	1	0.33	2	2
G	1	0.33	1	0.5	1	1	1	0.25	1	1
H	4	1	0.33	2	4	3	4	1	5	5
I	1	0.25	0.5	0.33	1	0.5	1	0.2	1	1
J	1	0.25	0.5	0.33	1	0.5	1	0.2	1	1

TABLE 21 Pairwise comparison of nodes with respect to trust

	A	B	C	D	E	F	G	H	I	J
A	1	3	2	4	3	1	5	6	1	2
B	0.33	1	1	1	1	0.5	1	3	0.25	1
C	0.5	1	1	2	1	0.5	3	4	0.33	1
D	0.25	1	0.5	1	1	0.333	1	2	0.2	0.5
E	0.33	1	1	1	1	0.5	2	3	0.25	1
F	1	2	2	3	0.2	1	4	5	0.5	1
G	2	1	0.33	1	0.5	0.25	1	1	0.16	0.33
H	0.16	0.33	0.25	0.5	0.33	0.2	1	1	0.14	0.25
I	1	4	3	5	4	2	5.99	7	1	3
J	0.5	1	1	2	1	1	3	4	0.333	1

2.3.3 | Weighted supermatrix

The eigenvectors obtained in unweighted supermatrix are transformed to weighted supermatrix to make it column stochastic, where the sum of each column is equal to 1, as presented in Table 23.

2.3.4 | Limit matrix

Limit matrix obtained by considering the weighted supermatrix to the power of $2k$ to achieve stable values, where k is arbitrary number to be considered. Limit matrix is the final matrix having the priority weights, as presented in Table 24. It consists the summary of the whole pairwise comparisons made. Limit matrix consists of the limit priority of all indirect relationships among elements. It shows the final weight of the nodes (alternatives) and criteria. Node having maximum priority weight is selected as phantom node. For instance, node I has the maximum weight; therefore, it is selected as phantom node, as presented in Table 24. Furthermore, the most important criteria can also be figured out from this matrix.

3 | RESULTS AND DISCUSSION

The whole process of ANP is repeated for all comparison between alternatives and criteria to get the limit matrix. It is the resultant matrix having the final priority weights used for decision making. The result shows that node I has the

TABLE 22 Unweighted supermatrix

		Alternatives										Criteria			
	B	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**Ac**	**Dist**	**Sp**	**Tr**
Alternatives	A	0	0	0	0	0	0	0	0	0	0	0.04	0.04	0.06	0.18
	B	0	0	0	0	0	0	0	0	0	0	0.1	0.16	0.18	0.06
	C	0	0	0	0	0	0	0	0	0	0	0.05	0.08	0.08	0.08
	D	0	0	0	0	0	0	0	0	0	0	0.05	0.05	0.12	0.05
	E	0	0	0	0	0	0	0	0	0	0	0.06	0.12	0.06	0.07
	F	0	0	0	0	0	0	0	0	0	0	0.05	0.05	0.08	0.13
	G	0	0	0	0	0	0	0	0	0	0	0.32	0.21	0.06	0.03
	H	0	0	0	0	0	0	0	0	0	0	0.13	0.16	0.23	0.02
	I	0	0	0	0	0	0	0	0	0	0	0.02	0.03	0.04	0.24
	J	0	0	0	0	0	0	0	0	0	0	0.13	0.04	0.04	0.09
Criteria	Ac	0.07	0.07	0.07	0.08	0.07	0.07	0.08	0.09	0.08	0.06	0	0	0	0
	Dist	0.1	0.17	0.17	0.14	0.2	0.21	0.21	0.14	0.12	0.19	0	0	0	0
	Sp	0.2	0.13	0.13	0.14	0.14	0.11	0.11	0.24	0.25	0.09	0	0	0	0
	Tr	0.6	0.6	0.6	0.62	0.56	0.59	0.58	0.51	0.53	0.63	0	0	0	0

TABLE 23 Weighted supermatrix

		Alternatives										Criteria			
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**Ac**	**Dist**	**Sp**	**Tr**
Alternatives	A	0	0	0	0	0	0	0	0	0	0	0.02	0.044	0.062	0.092
	B	0	0	0	0	0	0	0	0	0	0	0.052	0.169	0.181	0.033
	C	0	0	0	0	0	0	0	0	0	0	0.025	0.083	0.083	0.043
	D	0	0	0	0	0	0	0	0	0	0	0.025	0.057	0.124	0.025
	E	0	0	0	0	0	0	0	0	0	0	0.034	0.127	0.062	0.035
	F	0	0	0	0	0	0	0	0	0	0	0.025	0.057	0.083	0.069
	G	0	0	0	0	0	0	0	0	0	0	0.164	0.213	0.062	0.019
	H	0	0	0	0	0	0	0	0	0	0	0.068	0.169	0.238	0.013
	I	0	0	0	0	0	0	0	0	0	0	0.014	0.033	0.049	0.120
	J	0	0	0	0	0	0	0	0	0	0	0.068	0.044	0.049	0.046
Criteria	Ac	0.07	0.07	0.07	0.08	0.07	0.07	0.08	0.09	0.08	0.06	0	0	0	0
	Dist	0.1	0.17	0.17	0.14	0.2	0.21	0.21	0.14	0.12	0.19	0	0	0	0
	Sp	0.2	0.13	0.13	0.14	0.14	0.11	0.11	0.24	0.25	0.09	0	0	0	0
	Tr	0.6	0.6	0.6	0.62	0.56	0.59	0.58	0.51	0.53	0.63	0	0	0	0

maximum weight (ie, 0.128), thus selected as optimal node, as shown in Figure 3. Looking at Table 4, the trust level of node *I* is graded 9 and speed is 4, which means that trust is more important than speed in case of node *I*. In addition, node *I* is seven times more important than distance and eight times more important than acceleration.

Node *D* has the minimum weight (ie, 0.072), thus have low priority, as shown in Figure 3. In Table 4, the trust level of node *D* is graded 4 and speed is 7, which means that speed has moderate importance of trust. Moreover, trust value is of equal importance to distance because of having the same weights. Furthermore, trust value is equal or of slight importance than acceleration because node *D′s* trust value is 4 and acceleration is 3. Therefore, node *D′s* value is lower

TABLE 24 Limit matrix

		Alternatives										Criteria			
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**Ac**	**Dist**	**Sp**	**Tr**
Alternatives	A	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.043	0.043	0.043	0.043
	B	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.048	0.048	0.048	0.048
	C	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.032	0.032	0.032	0.032
	D	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.028	0.028	0.028	0.028
	E	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.032	0.032	0.032	0.032
	F	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.039	0.039	0.039	0.039
	G	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.042	0.042	0.042	0.042
	H	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.049	0.049	0.049	0.049
	I	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.050	0.050	0.050	0.050
	J	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.029	0.029	0.029	0.029
Criteria	Ac	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.064	0.064	0.064	0.064
	Dist	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.087	0.087	0.087	0.087
	Sp	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.106	0.106	0.106	0.106
	Tr	0.34	0.34	0.34	0.34	0.34	0.34	0.34	0.34	0.34	0.34	0.343	0.343	0.343	0.343

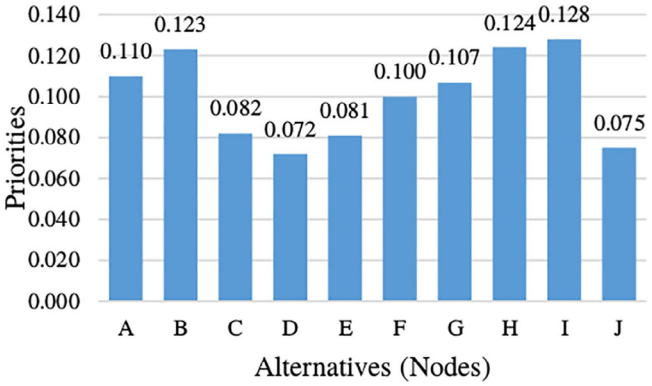

FIGURE 3 Nodes priorities

than other alternatives. All nodes are compared likewise with respect to given parameters. The results show that the proposed method can be used in decision making regarding the most optimal phantom node selection in the IoT-based VANETs.

Sensitivity analysis is performed to assess the steadiness of alternatives ranking. It is used to examine the outcomes and position of alternatives gained through the ANP model. In the weighted matrix, it is to be considered that the factors influence all elements in other options in criteria (parameters). For the stability (limit matrix), we examined node speed and its variation to test its impact on the overall score of the vehicles. The speed of each vehicle is analyzed from low, average, and high. In this way, the weights of the nodes changed, as shown in Figures 4 and 5. However, node I still have the highest score, which represents that the selection is optimal. Otherwise, a new vehicle will be selected. The sensitivity analysis can be performed with different scenarios and on all individual nodes.

4 | CONCLUSION

This article presents the problem of source location privacy preservation in urban areas having congested road intersections by selecting an optimal trusted phantom node using a multicriteria decision tool. The trusted phantom node selection depends on several parameters such as trust, speed, distance, and acceleration. The parameters and alternatives

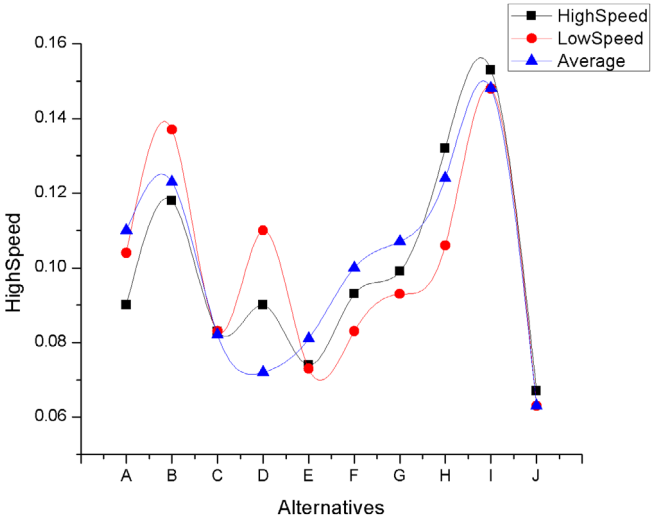

FIGURE 4 Sensitivity analysis with respect to high, low, and average speed of each vehicle

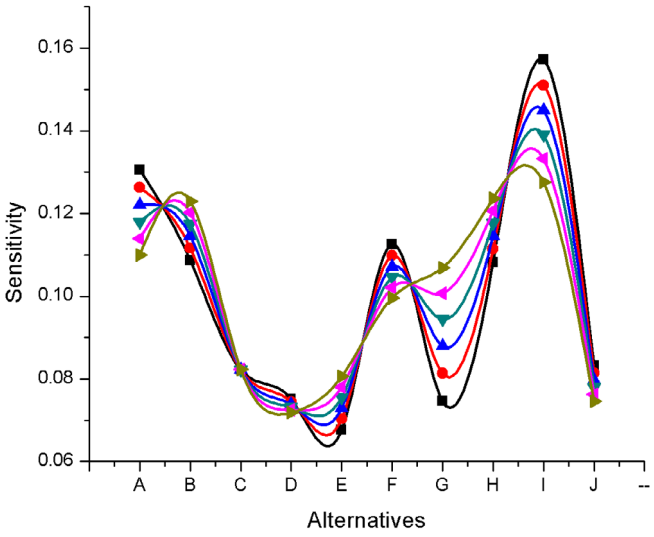

FIGURE 5 Sensitivity analysis with respect to speed

were pairwise compared using 9-point quantitative scale. The results show through limit matrix and sensitivity analysis that SESLPP selects an optimum trusted phantom node with highest priority weight. Limit matrix can also be used to optimize the criteria list and to identify the least important parameters. In the future, this work will be combined with existing phantom node selection techniques for different scenarios. Furthermore, it is expected to enhance the proposed technique by considering different parameters as well as different network scenarios in real time.

ACKNOWLEDGMENT

The work was supported by the Robotics and Internet-of-Things Lab of Prince Sultan University, Riyadh, Kingdom of Saudi Arabia.

ORCID

Abizar https://orcid.org/0000-0001-9472-6846
Zahid Khan https://orcid.org/0000-0003-4710-4010

REFERENCES

1. Papadimitratos P, Buttyan L, Holczer T, et al. Secure vehicular communication systems: design and architecture. arXiv preprint arXiv:0912.5391.
2. Martin-Vega FJ, Aguayo-Torres MC, Gomez G, Entrambasaguas JT, Duong TQ. Key technologies, modeling approaches, and challenges for millimeter-wave vehicular communications. *IEEE Commun Mag*. 2018;56(10):28-35.

3. Molina-Gil J, Caballero-Gil P, Caballero-Gil C. A vision of cooperation tools for VANETs. Paper presented at: 2010 IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM); IEEE; 2010:1-4.
4. Ros FJ, Ruiz PM, Stojmenovic I. Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks. *IEEE Trans Mob Comput*. 2012;11(1):33-46.
5. Khan Z, Fan P, A novel triple cluster based routing protocol (TCRP) for VANETs. Paper presented at: 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring); IEEE; 2016:1-5.
6. Khan Z, Fan P, Abbas F, Chen H, Fang S. Two-level cluster based routing scheme for 5G v2x communication. *IEEE Access*. 2019;7:16194-16205.
7. Khan Z, Fan P. A multi-hop moving zone (MMZ) clustering scheme based on cellular-v2x. *China Commun*. 2018;15(7):55-66.
8. Fonseca E, Festag A. A survey of existing approaches for secure ad hoc routing and their applicability to VANETs. *NEC Netw Lab*. 2006;28:1-28.
9. Sampigethaya K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K, Caravan: Providing location privacy for VANET. Tech. rep., Washington Univ Seattle Dept of Electrical Engineering; 2005.
10. Haghighi MS, Aziminejad Z. Highly anonymous mobility-tolerant location-based onion routing for VANETs. *IEEE IoT J*. 2019;1-1. https://doi.org/10.1109/JIOT.2019.2948315.
11. Bellur B. Certificate assignment strategies for a PKI-based security architecture in a vehicular network. Paper presented at: IEEE GLOBECOM 2008 - 2008 Global Telecommunications Conference; IEEE, 2008:1-6.
12. Farman H, Jan B, Talha M, et al. Multicriteria-based location privacy preservation in vehicular ad hoc networks. *Complexity*. 2018;1-12. https://doi.org/10.1155/2018/7697324.
13. Ma J, Yang C. A trust-based stable routing protocol in vehicular ad-hoc networks. *Int J Secur Appl*. 2015;9(4):107-116.
14. Huang Z, Ruj S, Cavenaghi MA, Stojmenovic M, Nayak A. A social network approach to trust management in VANETs. *Peer-to-Peer Netw Appl*. 2014;7(3):229-242.
15. Dotzer F, Fischer L, Magiera P. VARS: a vehicle ad-hoc network reputation system. Paper presented at: Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks; IEEE; 2005:454-456.
16. Ren Y, Boukerche A. Modeling and managing the trust for wireless and mobile ad hoc networks. Paper presented at: 2008 IEEE International Conference on Communications, ICC'08; IEEE; 2008:2129-2133
17. Sampigethaya K, Li M, Huang L, Poovendran R. Amoeba: robust location privacy scheme for VANET. *IEEE J Sel Areas Commun*. 2007;25(8):1569-1589.
18. Hafeez KA, Zhao L, Liao Z, Ma BN-W. Performance analysis of broadcast messages in VANETs safety applications. Paper presented at: 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010); IEEE; 2010:1-5.
19. Abedi O, Fathy M, Taghiloo J.S Enhancing AODV routing protocol using mobility parameters in VANET.
20. Satty TL. Decision making analytic hierarchy and network processes (AHP/ANP). *J Syst Sci Syst Eng*. 2004;13(1):1-35.
21. Lee H, Lee S, Park Y. Selection of technology acquisition mode using the analytic network process. *Math Comput Model*. 2009;49(5-6):1274-1282.
22. Hu Y-C. Analytic network process for pattern classification problems using genetic algorithms. *Inf Sci*. 2010;180(13):2528-2539.
23. Latif S, Mahfooz S, Jan B, et al. Multicriteria based next forwarder selection for data dissemination in vehicular ad hoc networks using analytical network process. *Math Probl Eng*. 2017;2017:1-18.
24. Farman H, Javed H, Jan B, et al. Analytical network process based optimum cluster head selection in wireless sensor network. *PLoS One*. 2017;12(7):e0180848.
25. Saaty TL. Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process. *RAC SAM*. 2008;102(2):251-318.
26. Nazir S, Anwar S, Khan SA, et al. Software component selection based on quality criteria using the analytic network process. *Abstract and Applied Analysis*. 2014;2014:1-12.

How to cite this article: Abizar, Farman H, Jan B, Khan Z, Koubaa A. A smart energy-based source location privacy preservation model for Internet of Things-based vehicular ad hoc networks. *Trans Emerging Tel Tech*. 2020;1–14. https://doi.org/10.1002/ett.3973