Hindawi
Complexity
Volume 2018, Article ID 7697324, 12 pages
https://doi.org/10.1155/2018/7697324

WILEY | Hindawi

Research Article

Multicriteria-Based Location Privacy Preservation in Vehicular Ad Hoc Networks

Haleem Farman,[1] **Bilal Jan**,[2] **Muhammad Talha**,[3] **Abi Zar**,[4] **Huma Javed**,[5] **Murad Khan**,[6] **Aziz Ud Din**,[7] **and Kijun Han**[8]

[1]*Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan*
[2]*Department of Computer Science, FATA University, FR Kohat, Pakistan*
[3]*Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia*
[4]*Faculty of Computer Science and IT, Universiti Malaysia Sarawak, Kota Samarahan, Malaysia*
[5]*Department of Computer Science, University of Peshawar, Peshawar, Pakistan*
[6]*Department of Computer Science & IT, Sarhad University of Science and IT, Peshawar, Pakistan*
[7]*Shiekh Zayed Islamic Center, University of Peshawar, Peshawar, Pakistan*
[8]*School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea*

Correspondence should be addressed to Kijun Han; kjhan@knu.ac.kr

Received 29 December 2017; Accepted 6 May 2018; Published 4 June 2018

Academic Editor: Danilo Comminiello

Vehicular ad hoc networks (VANETs) are the preferable choice for Intelligent Transportation Systems (ITS) because of its prevailing significance in both safety and nonsafety applications. Information dissemination in a multihop fashion along with privacy preservation of source node is a serious but challenging issue. We have used the idea of the phantom node as the next forwarder for data dissemination. The phantom node (vehicle) hides the identity of actual source node thus preserving the location privacy. The selection of the phantom node among the set of alternatives' candidate vehicles is considered as a multicriteria-based problem. The phantom node selection problem is solved by using an analytical network process (ANP) by considering different traffic scenarios. The selection is based on different parameters which are distance, speed, trust, acceleration, and direction. The best alternative (target phantom vehicle) is selected through an ANP where all the alternatives are ranked from best to worst. The vehicle having maximum weight is considered to be the best choice as a phantom node. In order to check the stability of the alternatives' ranking, sensitivity analysis is performed by taking into account different traffic scenarios and interest level of candidate vehicles.

1. Introduction

VANET is a network of vehicles to transfer information to each other directly or through fixed unit known as road side unit (RSU). The purpose of VANETs is to share safety and nonsafety messages such as weather information, entertainment, accidents, and monitoring of road traffic [1, 2]. Vehicles can directly communicate with each other known as vehicle-to-vehicle (V2V), while in vehicle to infrastructure (V2I), vehicles communicate with RSU. VANETs help Intelligent Transportation Systems (ITS) to provide safer, better, and more organized roads. The vehicles play an imperative role in our daily life. Every day, people spend considerable time on roads and feel stress while waiting in traffic jams that might result in road accidents. In order to make driving experiences safe, it is necessary to improve the transportation system by making it more reliable, effective, and proactive [3, 4]. Due to open nature of VANETs, privacy is considered as an important issue because vehicles try to communicate without disclosing their location details. The malicious performance of nodes, injecting false information, and changing and repeating messages could be harmful to other nodes. Moreover, the privacy-associated information of a node should be secure to avoid an observer from revealing actual identity

of a node, tracking their position, and concluding sensitive data. Protection and privacy guarantee benefits of enhanced driving. However, serious attacks may expose location privacy since an attacker could track routes of the concerned vehicle and obtain location information.

In literature, different efforts have been made to solve traffic problems to provide comfort to both drivers and passengers. Researchers in both industry and academia are making efforts to examine some key issues such as privacy preservation of the source vehicle and traffic monitoring. The focus of this paper is to preserve the location privacy of the source node, so that data transferring the location should not be shared with other vehicles in its communication range. The source node forwards data to the phantom node which is selected considering certain parameters such as distance, speed, acceleration, trust, and direction. Every time the source changes, it selects a new phantom node for communication, so that attacker may find it difficult to track the position of a source node.

In this paper, the selection of the phantom node is based on different parameters which makes it a multicriteria decision problem. Moreover, an analytical network process (ANP) [5] is used as a multicriteria decision tool. The ANP was introduced to solve the interdependencies and feedback between elements within a cluster or between the clusters. The ANP is suitable in those situations where parameters have dependencies on each other and need feedback as well. Here, we have used the ANP to select the optimal node as a trusted phantom node to address the dependencies of elements to come up with the most suitable option. Furthermore, ranking of the criteria and alternative elements will be determined for decision-making.

The rest of the paper is organized as follows. The overview of source location privacy in VANETs is discussed in Section 2; Section 3 is dedicated to multicriteria decision-making along with generic steps involved in an analytical network process. The phantom node selection using the analytical network process is explained in Section 4. Results and discussions are presented in Section 5, and finally, Section 6 concludes the paper with future directions.

2. Source Location Privacy in VANETs

Due to high congestion of automobiles on the roads, accidents are increasing day by day. Wireless technology is being used in vehicles to improve congestion by sending messages to share information with each other [6]. The advance technology of VANETs improves and enhances security and privacy of VANET communication and provides safety-related applications. Researchers have been devoted to resolve traffic problems and proposed various models. Existing techniques are based on group signature [7], pseudonymous [8], mix zones radio off [9], Efficient Conditional Privacy Preservation (ECPP) [10], AMOEBA [11], Communications Architecture for Reliable Adaptive Vehicular Ad Hoc Networks (CARAVAN) [12, 13], and so on. These methods are an effort to resolve many issues associated with location privacy in VANETs, but every method has its own limitation.

A number of pseudonymous base methods use public key infrastructure by using a digital signature for message authenticity, but the method involves imperative delay [14]. As stated that a 400 MHz processor equipped with the on-board unit (OBU) consumes about 20 ms to verify signature. This may cause significant delays in message verification in the dense urban area. Another drawback of pseudonymous base method is the certificate revocation list (CRL). Once a certificate authority (CA) administrator decides that a specific certificate should not be trusted anymore, the CA administrator can withdraw that certificate. The CA administrator publishes CRL to communicate the withdrawal of the certificate. The CA consumes time to track suspicious certificate and cancels the certificate in a long cancellation list.

Efficient Conditional Privacy Preservation (ECPP) [10] uses anonymous authentication for delivering safety messages with a certification authority and registration authority (RA) for traceability of vehicles. They have used RSUs (road side units) and on-board units (OBUs) which can deliver fast anonymous authentication in short time. A lot of storage capacity will be required for every OBU to accommodate anonymous key pairs in a large number. If some of OBUs anonymous keys are canceled, then every OBU updates the list that consumes long time.

AMOEBA [11] is based on group navigation of vehicles to protect location privacy. This technique is evaluated in expressways and highways in the presence of two passive adversary models, and various attacks are considered for testing robustness of user's privacy. A phenomenon is discussed in which a vehicle in a group of vehicles turns off its radio. In case the radio is switched off, then the vehicle will be cut off from the entire group and consequently would not be able to receive or send any messages.

Communications Architecture for Reliable Adaptive Vehicular Ad Hoc Networks (CARAVAN) [12, 13] uses spread spectrum with trusted computing platforms and a secret pseudorandom-spreading code. This code is used to prove the reliability of hardware and software of a distribution vehicle before permitting a vehicle to spread messages. The simulation result shows that CARAVAN produces message propagation latencies that are comparable to or better than less protected intervehicle communication protocols.

Another method to improve location privacy suggested for VANETs is based on pseudonyms [15]. In V2V communication, vehicles change their pseudonyms [16, 17] from time to time while broadcasting messages. Each message is comprised of the location, content, velocity, and time and is authenticated by signature by considering pseudonym. Different pseudonyms are used in routine by vehicles in VANETs. The vehicle location privacy can be ensured due to unlinkability of pseudonyms. However, if the pseudonym is changed by a vehicle in certain circumstances, adversary using old pseudonym can still link to the new pseudonym [18] and can monitor the whole link. Due to the information of velocity and location fixed in messages, the adversary can still guess to link the pseudonyms making privacy difficult.

The above discussed techniques have improved location privacy of the source node in VANETs, but still there is room

for more improvement by selecting a trusted node for privacy preservation. Therefore, in the proposed method, a trusted phantom node is selected to improve source location privacy using a multicriteria decision tool such as an ANP method. A multicriteria decision tool is being proposed because more than one parameter are involved which affect the selection of a trusted phantom node.

2.1. Adversary Model. In literature, different types of adversaries [19] are considered such as a global passive adversary (GPA), the restricted passive adversary (RPA), and local active adversary (LAA). The GPA and LAA are considered to be exterior observers which use a spectrum analyzer or angle of arrival to overhear the communication.

In the proposed model, a global passive adversary is assumed which is able to eavesdrop broadcasts of all vehicles and will be able to guess their locations. The actions of an adversary are such as injection of wrong information, hop by hop or backtracking through a spectrum analyzer or angle of arrival, and unnecessary message spreading. In addition, numerous types of attacks have also been identified and classified in the literature [20–25] on the basis of network layers used by attackers; their characteristics and intentions are mentioned in Table 1.

3. Multicriteria Decision-Making

The multicriteria decision-making (MCDM) is used where selection of elements are based on multiple factors that help in decision-making. In MCDM, on the basis of considered parameters, one element is selected among the available elements. In literature, different approaches are used to achieve the objective using different techniques such as the analytical network process (ANP) and analytical hierarchy process (AHP). In this paper, the ANP is used as it is widely used in literature in different fields such as software engineering, wireless sensor network (WSN), VANETS, and resource management [26–29]. In software engineering, an ANP is used for software component selection. The optimum cluster head selection in WSN based on ANP is proposed in [26]. The ANP has also been used for next forwarder vehicle selection to efficiently disseminate data in VANETs. The ANP scheme is briefly discussed in the following.

3.1. Analytical Network Process. The analytical network process is the enhanced version of analytical hierarchy process proposed by Saaty [30, 31]. The objective of the ANP is to deal with interdependency and feedback between elements within a cluster or among clusters. The ANP structures a given problem into network of clusters where each cluster has different components connected to each other. The general steps of the ANP are as follows:

(1) The first step is to formulate the problem, in which the problem is identified and divided into subproblems, if required. The objective is clearly defined along with the criteria (parameters) and alternatives (elements). Defining criteria/subcriteria is very important because the objective entirely depends on these parameters. On the basis of these parameters, alternatives are selected.

(2) Components in each cluster are pairwise compared, based on the quantitative scale proposed by Saaty [31] as presented in table. Each element is scaled according to its importance over other elements by considering certain parameter. A matrix is generated against each comparison made, where 1 is of equal importance while 9 represents the most importance.

(3) Local priorities are assigned to each comparison and every individual comparison matrix is represented through eigenvector to get the normalized weights.

(4) It is very important to check the reliability of each comparison made. In order to do so, Saaty [31] proposed the consistency ratio (CR), which defines how much of the comparison made is consistent. The CR needs to be equal to or less than 0.1, which means that inconsistency is allowed up to 10%. If it exceeds, the comparison need to be revised.

(5) The outcome of all the comparison matrix is combined into unweighted supermatrix. These local priorities are transformed into weighted supermatrix by making it column stochastic.

(6) The weighted supermatrix is transformed into limit matrix by raising it to the power of $2k$ to get more stable values, where k is any arbitrary number. Limit matrix is the resultant matrix, containing final weight of each element. It determines the best alternative and most important criteria as well.

(7) Sensitivity check is performed to determine the stability of alternatives' ranking.

4. Phantom Node Selection Using an ANP Model

The location of the source is very important in VANETs; therefore, it is important to preserve privacy of a node. In this paper, an ANP model is used to select the phantom node to preserve privacy of the source location. The proposed technique considers V2V infrastructure in which vehicles directly communicate with each other. Source node communicates through a trusted phantom node, which is based on certain parameters such as trust, speed, distance, acceleration, and direction, as presented in Table 2. Every time, the source selects a different phantom node for communication, so that it is difficult for the attacker to track the position of the source. The selected node acts as a phantom node that forwards messages to improve source location privacy within its communication range.

In the proposed network scenario as shown in Figure 1, in order to forward data, a source node sends a packet to a phantom node. The phantom node is selected on the basis of trust, distance, speed, acceleration, and direction. Trust [32] indicates the confidence of a node over another node in a network. Distance [11, 33] can be measured between

Table 1: Attacks and their characteristics.

Attack	Consequences	Type	Effects
Bogus information	Fake information injection	Insider	Authentication
ID disclosure	Monitoring routes and changing ID of the vehicle	Insider/passive	Privacy
Denial of service	Transfer unnecessary messages on the channel	Local/active	Availability
Replaying and dropping packets	Drop and delay of packets	Insider/active	Authentication
Hidden vehicle	Decrease the congestion on the wireless channel	Outsider/passive	Privacy

Table 2: Parameter description.

Parameters	Description
SN	Source node
PN	Phantom node
TL	Trust level
SL	Speed level
DL	Distance level
Ac	Acceleration
Dr	Direction

the source and phantom node in meters, while speed [11] can be defined as the rate of movement of a vehicle in a network. Acceleration is considered as the rate of change of velocity of a vehicle with respect to time [11, 34]. We have considered direction as well, because it is very important to determine the direction of the source node to the phantom node. The node in the opposite direction will have low priority as compared to the one in the same direction. A source node selects the phantom node within its communication range as shown in Algorithm 1. The selection of the phantom node using an ANP is explained.

4.1. Problem Identification. The identified problem is structured into goal, criteria, and alternatives. In this paper, goal is to select the optimal vehicle as a phantom node, based on five given criteria (parameters). Alternatives are the vehicles upon which has to be made. In problem formulation, criteria selection is very important as the decision is based on these parameters. Once all the parameters and alternatives are identified, each element of criteria cluster is compared with every element of alternative cluster and vice versa.

4.2. Pairwise Comparison. In pairwise comparison, the importance of elements in one cluster is judged in accordance with the elements of another cluster. Each comparison is assigned with a local weight and represented through matrix. These weights must be carefully assigned as the decision mainly depends on these comparisons. The elements of criteria and alternative clusters are compared with each other, according to the 9-point quantitative scale, 1 represents equal importance where 9 for the high priority. Elements compared with itself have equal importance, hence represented by 1 as shown in matrix (3).

4.2.1. Criteria Comparison with respect to Alternatives. Each element of criteria cluster is pairwise compared with respect to each alternative according to Table 3. The resultant of all comparison is the comparison matrix, which includes all the comparisons made as shown in matrix (4). The values above diagonal are obtained from pairwise comparison where below values are the reciprocal of these comparisons. For instance, in the proposed scenario as shown in Figure 1, V1 is considered for all elements in criteria. Matrix (4) is the resultant of all comparisons of elements in criteria for V1. Each column obtained in matrix (4) is summed up, and each individual value is divided by its corresponding column total as shown in matrix (5). Afterwards, the average of each individual row is considered as eigenvector (EV). To check the reliability of pairwise comparison, the consistency ratio (CR) is calculated. According to Saaty [31], CR must be equal to or less than 0.1, otherwise pairwise comparison needs to be revised. The CR can be calculated using (1), where CI is the consistency index and RI is the random index. CI can be obtained using (2), and the value of RI can be determined using Table 4 [31]. The CR for V1 is 0.08 as shown in matrix (6).

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}}, \tag{1}$$

$$\mathrm{CI} = \frac{\lambda\,\max - n}{n-1}, \tag{2}$$

$$\begin{bmatrix} & A & D & S & T & \mathrm{Dr} \\ A & 1 & & & & \\ D & & 1 & & & \\ S & & & 1 & & \\ T & & & & 1 & \\ \mathrm{Dr} & & & & & 1 \end{bmatrix}, \tag{3}$$

$$\begin{bmatrix} & \mathrm{Ac} & \mathrm{Dr} & \mathrm{DL} & \mathrm{SL} & \mathrm{TL} \\ \mathrm{Ac} & 1 & 0.33 & 0.5 & 0.33 & 0.2 \\ \mathrm{Dr} & 3.0 & 1 & 3.0 & 4.0 & 0.33 \\ \mathrm{DL} & 2.0 & 0.33 & 1 & 0.33 & 0.2 \\ \mathrm{SL} & 3.0 & 0.25 & 3.0 & 1 & 0.2 \\ \mathrm{TL} & 5.0 & 3.0 & 5.0 & 5.0 & 1 \end{bmatrix}, \tag{4}$$

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} \\ \text{Ac} & \frac{1}{14}=0.07 & \frac{0.33}{4.91}=0.06 & \frac{0.5}{12.5}=0.04 & \frac{0.33}{10.6}=0.03 & \frac{0.2}{1.93}=0.1 \\ \text{Dr} & \frac{3.0}{14}=0.21 & \frac{1}{4.91}=0.203 & \frac{3.0}{12.5}=0.24 & \frac{4.0}{10.6}=0.37 & \frac{0.33}{1.93}=0.17 \\ \text{DL} & \frac{2.0}{14}=0.14 & \frac{0.33}{4.91}=0.06 & \frac{1}{12.5}=0.08 & \frac{0.33}{10.6}=0.03 & \frac{0.2}{1.93}=0.1 \\ \text{SL} & \frac{3.0}{14}=0.21 & \frac{0.25}{4.91}=0.05 & \frac{3.0}{12.5}=0.24 & \frac{1}{10.6}=0.09 & \frac{0.2}{1.93}=0.1 \\ \text{TL} & \frac{5.0}{14}=0.35 & \frac{3.0}{4.91}=0.61 & \frac{5.0}{12.5}=0.4 & \frac{5.0}{10.6}=0.47 & \frac{1}{1.93}=0.52 \end{bmatrix}, \tag{5}$$

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} & \text{EV} \\ \text{Ac} & 0.07 & 0.06 & 0.04 & 0.03 & 0.10 & 0.06 \\ \text{Dr} & 0.21 & 0.20 & 0.24 & 0.37 & 0.17 & 0.24 \\ \text{DL} & 0.14 & 0.06 & 0.08 & 0.03 & 0.1 & 0.08 \\ \text{SL} & 0.21 & 0.05 & 0.24 & 0.09 & 0.1 & 0.14 \\ \text{TL} & 0.35 & 0.61 & 0.40 & 0.47 & 0.52 & 0.47 \\ \text{CR} = 0.08 & & & & & & \end{bmatrix}. \tag{6}$$

The remaining matrices (7) and (8) are obtained using same process. The value of CR of all matrices must be less than 0.1. In matrix (7), elements in criteria are compared with respect to V2, V3, V4, V5, V6, and V7, respectively.

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} \\ \text{Ac} & 1 & 0.33 & 0.5 & 0.33 & 0.2 \\ \text{Dr} & 3.0 & 1 & 3.0 & 3.0 & 0.33 \\ \text{DL} & 2.0 & 0.33 & 1 & 2.0 & 0.2 \\ \text{SL} & 3.0 & 0.33 & 0.5 & 1 & 0.2 \\ \text{TL} & 5.0 & 3.0 & 5.0 & 5.0 & 1 \\ \text{CR} = 0.06 & & & & & \end{bmatrix},$$

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} \\ \text{Ac} & 1 & 0.33 & 0.5 & 0.33 & 0.2 \\ \text{Dr} & 3.0 & 1 & 3.0 & 4.0 & 0.25 \\ \text{DL} & 2.0 & 0.33 & 1 & 2.0 & 0.2 \\ \text{SL} & 3.0 & 0.25 & 0.5 & 1 & 0.2 \\ \text{TL} & 5.0 & 4.0 & 5.0 & 5.0 & 1 \\ \text{CR} = 0.08 & & & & & \end{bmatrix},$$

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} \\ \text{Ac} & 1 & 0.33 & 0.5 & 0.5 & 0.2 \\ \text{Dr} & 3.0 & 1 & 3.0 & 3.0 & 0.25 \\ \text{DL} & 2.0 & 0.33 & 1 & 1.0 & 0.2 \\ \text{SL} & 2.0 & 0.33 & 1.0 & 1 & 0.2 \\ \text{TL} & 5.0 & 4.0 & 5.0 & 5.0 & 1 \\ \text{CR} = 0.03 & & & & & \end{bmatrix},$$

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} \\ \text{Ac} & 1 & 0.33 & 0.33 & 0.33 & 0.2 \\ \text{Dr} & 3.0 & 1 & 4.0 & 3.0 & 0.25 \\ \text{DL} & 3.0 & 0.25 & 1 & 2.0 & 0.25 \\ \text{SL} & 3.0 & 0.33 & 0.5 & 1 & 0.25 \\ \text{TL} & 5.0 & 4.0 & 4.0 & 4.0 & 1 \\ \text{CR} = 0.09 & & & & & \end{bmatrix},$$

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} \\ \text{Ac} & 1 & 0.25 & 0.33 & 0.5 & 0.2 \\ \text{Dr} & 4.0 & 1 & 3.0 & 4.0 & 0.2 \\ \text{DL} & 3.0 & 0.33 & 1 & 3.0 & 0.2 \\ \text{SL} & 2.0 & 0.25 & 0.33 & 1 & 0.25 \\ \text{TL} & 5.0 & 5.0 & 5.0 & 4.0 & 1 \\ \text{CR} = 0.1 & & & & & \end{bmatrix},$$

$$\begin{bmatrix} & \text{Ac} & \text{Dr} & \text{DL} & \text{SL} & \text{TL} \\ \text{Ac} & 1 & 0.33 & 0.5 & 0.5 & 0.2 \\ \text{Dr} & 3.0 & 1 & 4.0 & 3.0 & 0.25 \\ \text{DL} & 2.0 & 0.25 & 1 & 3.0 & 0.25 \\ \text{SL} & 2.0 & 0.33 & 0.33 & 1 & 0.2 \\ \text{TL} & 5.0 & 4.0 & 4.0 & 5.0 & 1 \\ \text{CR} = 0.08 & & & & & \end{bmatrix}. \tag{7}$$

4.2.2. Alternatives' Comparison with respect to Criteria. The elements in alternatives (V1 to V7) are compared with respect to every individual element in criteria cluster as shown in matrix (8) in order of acceleration, distance, speed, trust, and direction, respectively.

	V1	V2	V3	V4	V5	V6	V7
V1	1	2.0	0.33	2.0	0.5	2.0	0.14
V2	0.5	1.0	2.0	2.0	1.0	2.0	0.25
V3	3.0	0.5	1.0	1.0	2.0	2.0	0.25
V4	0.5	0.5	1.0	1.0	0.5	2.0	0.25
V5	2.0	1.0	0.5	2.0	1.0	1.0	0.25
V6	0.5	0.5	0.5	0.5	1.0	1.0	0.25
V7	7.0	4.0	4.0	4.0	4.0	4.0	1.0
CR =	0.08						

,

	V1	V2	V3	V4	V5	V6	V7
V1	1	0.25	0.5	1.0	0.33	1.0	0.20
V2	4.0	1.0	2.0	3.0	1.0	3.0	0.50
V3	2.0	0.5	1.0	2.0	2.0	1.0	0.33
V4	1.0	0.33	0.5	1.0	0.5	1.0	0.25
V5	3.0	1.0	0.5	2.0	1.0	2.0	0.50
V6	1.0	0.33	1.0	1.0	0.5	1.0	0.25
V7	5.0	2.0	3.0	4.0	2.0	4.0	1.0
CR =	0.02						

,

	V1	V2	V3	V4	V5	V6	V7
V1	1.0	0.5	0.33	0.5	1.0	1.0	0.33
V2	2.0	1.0	2.0	1.0	3.0	2.0	3.0
V3	3.0	0.5	1.0	1.0	1.0	1.0	1.0
V4	2.0	1.0	1.0	1.0	2.0	1.0	2.0
V5	1.0	0.33	1.0	0.5	1.0	1.0	1.0
V6	1.0	0.5	1.0	1.0	1.0	1.0	1.0
V7	3.0	0.33	1.0	0.5	1.0	1.0	1.0
CR =	0.03						

,

	V1	V2	V3	V4	V5	V6	V7
V1	1.0	3.0	2.0	4.0	3.0	0.5	2.0
V2	0.33	1.0	0.5	2.0	1.0	0.33	0.33
V3	0.5	2.0	1.0	3.0	3.0	0.5	2.0
V4	0.25	0.5	0.33	1.0	0.5	0.33	0.5
V5	0.33	1.0	0.33	2.0	1.0	0.33	0.25
V6	2.0	3.0	2.0	3.0	3.0	1.0	3.0
V7	0.5	3.0	0.5	2.0	4.0	0.33	1.0
CR =	0.04						

,

	V1	V2	V3	V4	V5	V6	V7
V1	1.0	1.0	0.14	0.16	0.2	0.16	3.0
V2	1.0	1.0	0.14	0.2	0.16	0.16	5.0
V3	7.0	7.0	1.0	3.0	4.0	4.0	7.0
V4	6.0	5.0	0.33	1.0	3.0	3.0	7.0
V5	5.0	6.0	0.25	0.33	1.0	3.0	6.0
V6	6.0	6.0	0.25	0.33	0.33	1.0	6.0
V7	0.33	0.2	0.14	0.14	0.16	0.16	1.0
CR =	0.10						

.

(8)

4.3. Unweighted and Weighted Supermatrix. The EV obtained in matrices (6), (7), (8) are combined and represented in unweighted supermatrix as shown in Table 5. It contains the local weights obtained through pairwise comparisons. It is then transformed into weighted supermatrix, where the sum of each column is 1 as shown in Table 6.

5. Results and Discussions

In this section, the results are thoroughly discussed taking into account the ANP major steps (discussed in Section 4) and outcome of each step. The outcome of the ANP model is limit matrix, which provides insight for best alternative and criteria. Alongside, sensitivity analysis has been performed to check the stability of these alternatives and the impact of criteria on it.

5.1. Limit Matrix. Limit matrix is the resultant matrix, which contains the final weights against each element in criteria and alternative clusters. It is obtained from the weighted supermatrix in which the values are raised to the power of $2k$ to get same value for each row, where k is any random number. Table 7 represents limit matrix, on the basis of which decision can be made. Figure 2 illustrates that V6 has the high weight; therefore, it is the most suitable vehicle to be selected as a phantom node, followed by V3 and so on. The most important criteria can also be determined from limit matrix. Here, trust parameter has high priority score, followed by direction and so on. Therefore, we can conclude that V6 is the best choice among all vehicles, and trust is the most important parameter. Moreover, parameters can be prioritized using an ANP model. The parameter having very small value can be eliminated to overcome computational overhead. To check the stability of the alternative ranking, we performed sensitivity check.

5.2. Sensitivity Analysis. It is necessary to check the stability of the alternative rankings obtained through limit matrix. In order to do so, the sensitivity analysis is performed. It is highly recommended but not mandatory. The objective of this test is to check how much of the ranking of alternative will be influenced by the elements in criteria cluster. Element having higher weight is considered, and its impact on all

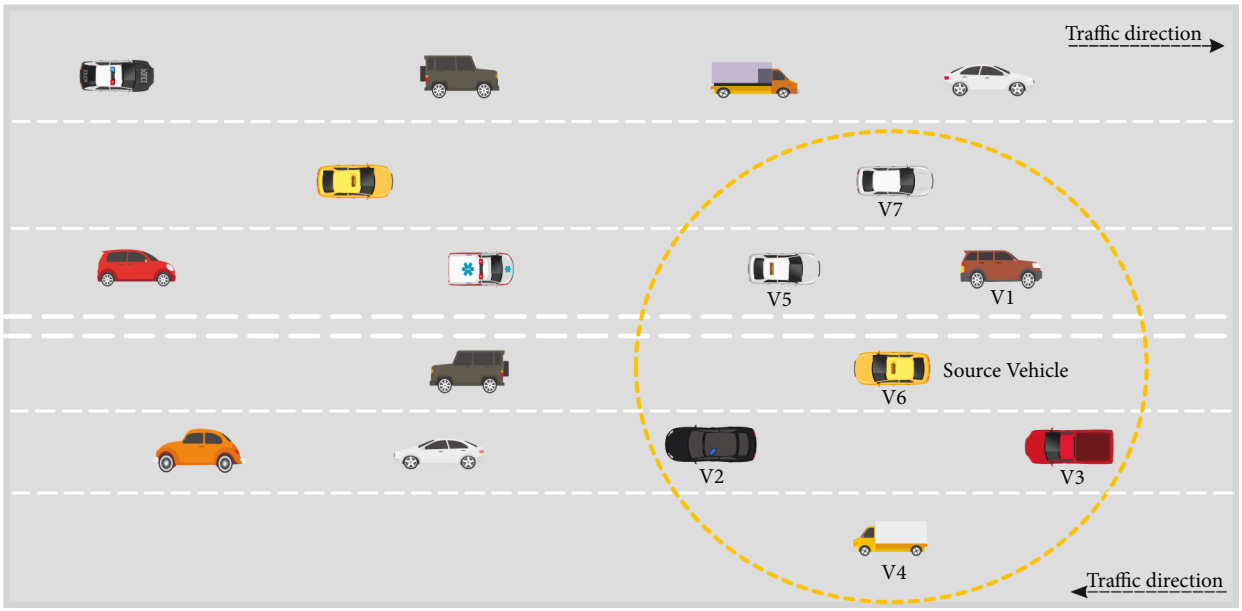

Figure 1: Proposed scenario.

1. Initialization phase
2. Source node starts transmission
   Next hop = null
3. **While** (next hop =! Phantom node)
   ANP process is executed for all possible comparison
   Select phantom node
   If (next hop = update)
   Phantom node = update
   PN = Ac + TL + SL + AL + DL + Dr
   \\PN is determined using alternative ranking
   Else
   Broadcast beacon message
4. **end**

Algorithm 1: (phantom node selection).

Table 3: the 9-point quantitative scale.

Scale	Description
1	Equal relative importance
2	Equally to moderately more important
3	Moderately more important
4	Moderately to strongly important
5	Strongly important
6	Strongly to very strongly more important
7	Very strongly more important
8	Very strongly to extremely more important
9	Extremely important of high priority

Table 4: Random consistency index.

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.52	0.89	1.11	1.25	1.35	1.40	1.45

elements in alternative ranking is determined. Here, trust parameter has the high weight, but we have considered direction for sensitivity analysis as we want to restrict the dissemination of information (accident, weather, and entertainment) only to vehicles of interest. In order to check the impact of parameters on the alternatives, we have considered two different scenarios.

5.2.1. Scenario 1. In first scenario, all nodes in the interference region of the source vehicle are considered as interested vehicles (Figure 1), to whom information (weather or entertainment) has to be communicated. In this scenario, based on parameters (already discussed in section 4) V6 has the maximum weight computed through an ANP model and therefore is the optimum choice to be a phantom node. The sensitivity analysis is performed in order to check the stability of the alternative ranking. In Figure 3, V6 is the best choice for selection as a phantom node, as it has the maximum weight, followed by V3 with weight slightly less than V6, thus making V3 the second most suitable choice. The y-axis shows the weights obtained by every vehicle, and x-axis represents the phantom node selection weights.

5.2.2. Scenario 2. This subsection provides an optimized solution to the problem of phantom node selection based on the interest region of the source vehicle. In the first step, vehicles inside the interference region of the source node are classified as *interested* and *noninterested* vehicles based on effectiveness of criteria parameters. In the second step, the whole ANP is revised, where the pairwise comparison is made in

Table 5: Unweighted supermatrix.

		Alternatives							Criteria				
		V1	V2	V3	V4	V5	V6	V7	Ac	Dr	DL	SL	TL
Alternatives	V1	0	0	0	0	0	0	0	0.1007	0.0454	0.0600	0.0833	0.2190
	V2	0	0	0	0	0	0	0	0.1195	0.0533	0.2003	0.2467	0.0741
	V3	0	0	0	0	0	0	0	0.1311	0.3108	0.133	0.1429	0.1644
	V4	0	0	0	0	0	0	0	0.0777	0.2493	0.0679	0.1795	0.0540
	V5	0	0	0	0	0	0	0	0.1054	0.1825	0.1442	0.1021	0.0688
	V6	0	0	0	0	0	0	0	0.0628	0.1265	0.0771	0.1201	0.2794
	V7	0	0	0	0	0	0	0	0.4024	0.0319	0.3170	0.1250	0.14
Criteria	Ac	0.0599	0.0624	0.0604	0.0657	0.0564	0.0537	0.0637	0	0	0	0	0
	Dr	0.2510	0.2332	0.2294	0.2184	0.2421	0.224	0.2390	0	0	0	0	0
	DL	0.0783	0.1165	0.1100	0.0972	0.1229	0.1267	0.1246	0	0	0	0	0
	SL	0.1310	0.0986	0.0906	0.0972	0.0974	0.0752	0.0790	0	0	0	0	0
	TL	0.4796	0.4890	0.5094	0.5213	0.481	0.5203	0.4935	0	0	0	0	0

Table 6: Weighted supermatrix.

		Alternatives							Criteria				
		V1	V2	V3	V4	V5	V6	V7	Ac	Dr	DL	SL	TL
Alternatives	V1	0	0	0	0	0	0	0	0.100	0.045	0.060	0.083	0.219
	V2	0	0	0	0	0	0	0	0.119	0.053	0.200	0.246	0.074
	V3	0	0	0	0	0	0	0	0.131	0.310	0.133	0.142	0.164
	V4	0	0	0	0	0	0	0	0.077	0.249	0.067	0.179	0.054
	V5	0	0	0	0	0	0	0	0.105	0.182	0.144	0.102	0.068
	V6	0	0	0	0	0	0	0	0.062	0.126	0.077	0.120	0.279
	V7	0	0	0	0	0	0	0	0.402	0.031	0.317	0.125	0.14
Criteria	Ac	0.059	0.062	0.060	0.065	0.056	0.053	0.063	0	0	0	0	0
	Dr	0.251	0.233	0.229	0.218	0.242	0.224	0.239	0	0	0	0	0
	DL	0.078	0.116	0.110	0.097	0.122	0.126	0.124	0	0	0	0	0
	SL	0.131	0.098	0.090	0.097	0.097	0.075	0.079	0	0	0	0	0
	TL	0.479	0.489	0.509	0.521	0.481	0.520	0.493	0	0	0	0	0

Table 7: Limit matrix.

		Alternatives							Criteria				
		V1	V2	V3	V4	V5	V6	V7	Ac	Dr	DL	SL	TL
Alternatives	V1	0.0704	0.0704	0.0704	0.0704	0.0704	0.0704	0.0704	0.0704	0.0704	0.0704	0.0704	0.0704
	V2	0.0511	0.0511	0.0511	0.0511	0.0511	0.0511	0.0511	0.0511	0.0511	0.0511	0.0516	0.0511
	V3	0.0955	0.0955	0.0955	0.0955	0.0955	0.0955	0.0955	0.0955	0.0955	0.0955	0.0955	0.0955
	V4	0.0572	0.0572	0.0572	0.0572	0.0572	0.0572	0.0572	0.0572	0.0572	0.0572	0.0572	0.0572
	V5	0.0545	0.0545	0.0545	0.0545	0.0545	0.0545	0.0545	0.0545	0.0545	0.0545	0.0545	0.0545
	V6	0.0966	0.0966	0.0966	0.0966	0.0966	0.0966	0.0966	0.0966	0.0966	0.0966	0.0966	0.0966
	V7	0.0744	0.0744	0.0744	0.0744	0.0744	0.0744	0.0744	0.0744	0.0744	0.0744	0.0744	0.0744
Criteria	Ac	0.0299	0.0299	0.0299	0.0299	0.0299	0.0299	0.0299	0.0299	0.0299	0.0299	0.0299	0.0299
	Dr	0.1166	0.1166	0.1166	0.1166	0.1166	0.1166	0.1166	0.1166	0.1166	0.1166	0.1166	0.1166
	DL	0.055	0.0558	0.0558	0.0558	0.0558	0.0558	0.0558	0.0558	0.0558	0.0558	0.0558	0.0558
	SL	0.0469	0.0469	0.0469	0.0469	0.0469	0.0469	0.0469	0.0469	0.0469	0.0469	0.0469	0.0469
	TL	0.2505	0.2505	0.2505	0.2505	0.2505	0.2505	0.2505	0.2505	0.2505	0.2505	0.2505	0.2505

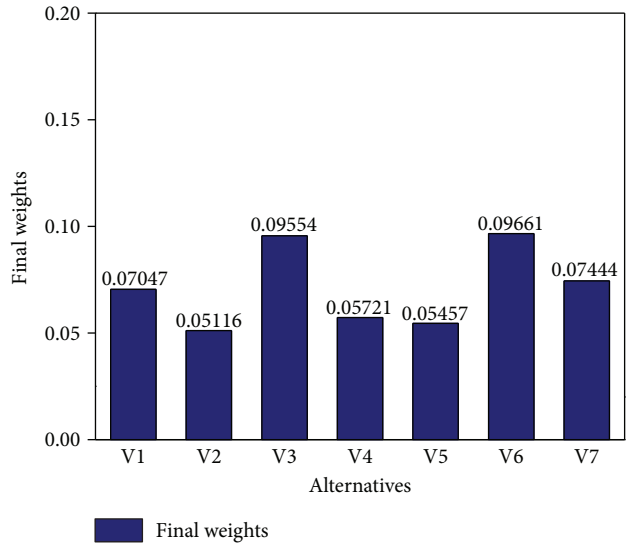

Figure 2: Final weights of elements in alternative cluster.

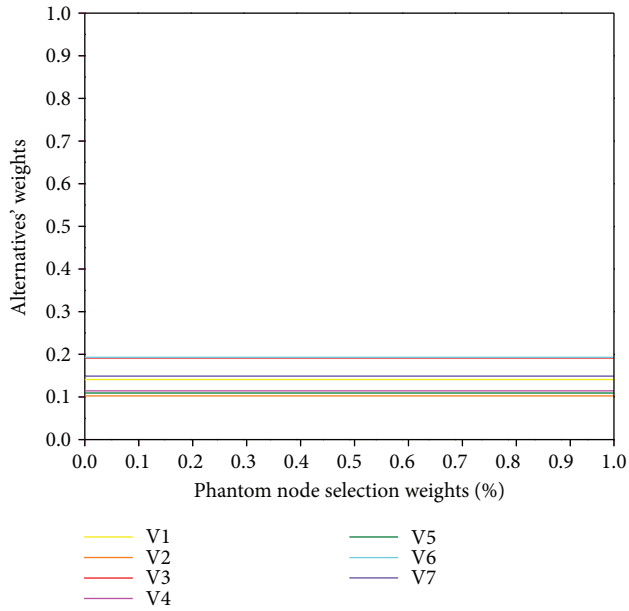

Figure 3: Scenario 1.

accordance with the importance of chosen criteria parameters. Less important criteria parameters are either omitted or given less weightage in the ANP. In the third step, the alternative ranking is determined. In last step, the sensitivity analysis is performed and the impact of criteria parameter is determined on the optimized alternative ranking. For instance, the accident has occurred in the separate lane; therefore, the vehicles in the opposite lane are not considered as they are moving in the opposite direction. The less interested vehicles in the interference region of the source node are shown in the shaded region (Figure 4). Therefore, the traffic flow on the opposite lane should not be affected as shown in Figure 4. The sensitivity analysis is presented in Figure 5, where V3 is the best alternative to be selected for the phantom node.

6. Conclusion and Future Directions

In this paper, the goal is to select the optimal trusted node (vehicle) that can preserve location privacy of the source node in VANETs. The selection of the phantom node is based on different parameters which are distance, speed, trust, acceleration, and direction that makes it a multicriteria decision problem. Analytical network process has been used to deal with such problem. The goal, criteria, and alternatives are identified first, and then each element of criteria is

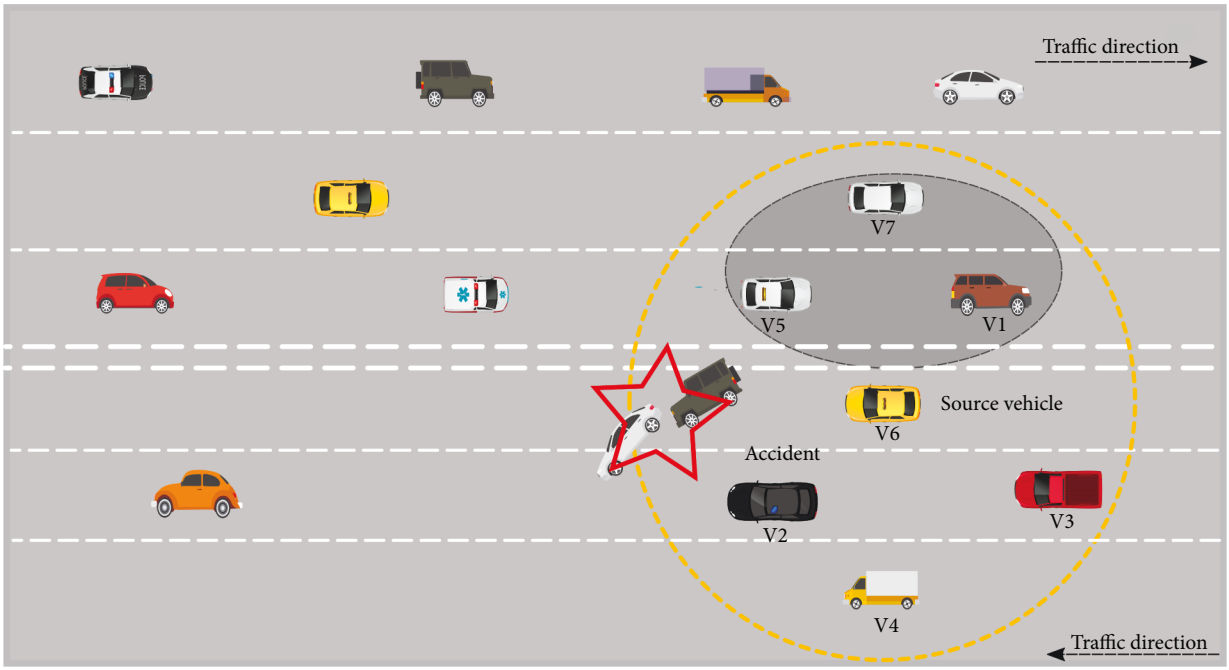

Figure 4: Information dissemination to vehicles in the interest zone only.

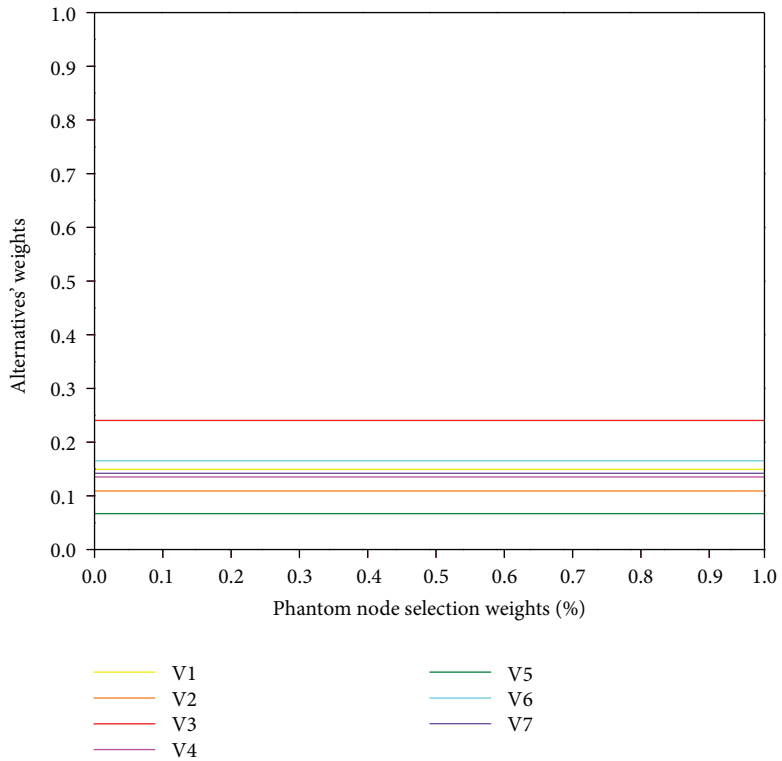

Figure 5: Scenario 2.

pairwise compared with all elements of alternatives and vice versa. The whole process of an ANP is concluded in limit matrix which presents the best alternative and most important criteria. The proposed method is tested on two different scenarios in order to check the stability of the alternatives' ranking. Scenario 1 is for nonsafety events such as weather information and entertainment, in which information is disseminated to all vehicles that are in the range of the phantom node. Among all the alternatives, V6 has high weights and considered to be the best choice for the phantom node. Safety

application is considered in scenario 2, where an accident occurs on one specific lane. The whole process of an ANP is applied and then tested for sensitivity analysis. Vehicles moving in the opposite direction are of least interest to this event and therefore given less priority. Results illustrate that the vehicles which are in the opposite direction to the source node are of less interest to the one that move in the same direction. In the future, we will extend this work by considering different highways and urban scenarios.

Conflicts of Interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors are grateful to the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia, for funding this project through research group Project no. RG-1437-37. This work was supported by Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korean Government (MSIP) (no. 2017-0-00770). This study was supported by the BK21 plus project (SW Human Resource Development Program for supporting Smart life) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (21A20131600005).

References

[1] S. Latif, S. Mahfooz, B. Jan, N. Ahmad, Y. Cao, and M. Asif, "A comparative study of scenario-driven multi-hop broadcast protocols for VANETs," *Vehicular Communications*, vol. 12, pp. 88–109, 2018.

[2] P. Papadimitratos, L. Buttyan, T. Holczer et al., "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[3] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 1, pp. 33–46, 2012.

[4] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS," *NEC Network Laboratories*, vol. 28, pp. 1–28, 2006.

[5] T. L. Saaty, "Decision making — the Analytic Hierarchy and Network Processes (AHP/ANP)," *Journal of Systems Science and Systems Engineering*, vol. 13, no. 1, pp. 1–35, 2004.

[6] S. H. Bouk, G. Kim, S. H. Ahmed, and D. Kim, "Hybrid adaptive beaconing in vehicular ad hoc networks: a survey," *International Journal of Distributed Sensor Networks*, vol. 11, no. 5, Article ID 390360, 2015.

[7] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[8] B. Bellur, "Certificate assignment strategies for a PKI-based security architecture in a vehicular network," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, pp. 1–6, New Orleans, LO, USA, November-December 2008.

[9] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93–105, 2016.

[10] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pp. 1229–1237, Phoenix, AZ, USA, April 2008.

[11] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[12] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, *CARAVAN: Providing Location Privacy for VANET*, Washington Univ Seattle Dept of Electrical Engineering, 2005.

[13] J. J. Blum and A. Eskandarian, "Fast, robust message forwarding for inter-vehicle communication netw," in *2006 IEEE Intelligent Transportation Systems Conference*, pp. 1418–1423, Toronto, Ont., Canada, September 2006.

[14] H.-C. Hsiao, A. Studer, C. Chen et al., "Flooding-resilient broadcast authentication for VANETs," in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking - MobiCom '11*, pp. 193–204, Las Vegas, Nevada, USA, September 2011.

[15] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks - VANET '07*, pp. 19–28, Montreal, Quebec, Canada, September 2007.

[16] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J. P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, Vancouver, BC, Canada, 2007.

[17] A. R. Beresford and F. Stajano, "Mix zones: user privacy in location-aware services," in *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*, pp. 127–131, Orlando, FL, USA, USA, March 2004.

[18] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160–171, 2010.

[19] M. A. Moharrum and A. A. Al Daraiseh, "Toward secure vehicular ad-hoc networks: a survey," *IETE Technical Review*, vol. 29, no. 1, pp. 80–89, 2012.

[20] V. Balakrishnan, V. Varadharajan, U. Tupakula, and P. Lucs, "TEAM: trust enhanced security architecture for mobile ad-hoc networks," in *2007 15th IEEE International Conference on Networks*, pp. 182–187, Adelaide, SA, Australia, November 2007.

[21] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET," in *2009 Second International Workshop on Computer Science and Engineering*, vol. 2, pp. 160–165, Qingdao, China, October 2009.

[22] M. Rahbari and M. A. J. Jamali, "Efficient detection of Sybil attack based on cryptography in VANET," 2011, http://arxiv.org/abs/1112.2257.

[23] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, "A Sybil attack detection approach using neighboring vehicles in VANET," in *Proceedings of the 4th International Conference on Security of Information and Networks - SIN '11*, pp. 151–158, Sydney, Australia, November 2011.

[24] S. G. Najafabadi, H. R. Naji, and A. Mahani, "Sybil attack detection: improving security of WSNs for smart power grid application," in *2013 Smart Grid Conference (SGC)*, pp. 273–278, Tehran, Iran, December 2013.

[25] V. Hoa la and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey," *International Journal on AdHoc Networking Systems*, vol. 4, no. 2, pp. 1–20, 2014.

[26] H. Farman, H. Javed, B. Jan et al., "Analytical network process based optimum cluster head selection in wireless sensor network," *PLoS One*, vol. 12, no. 7, article e0180848, 2017.

[27] S. Nazir, S. Shahzad, R. B. Atan, and H. Farman, "Estimation of software features based birthmark," *Cluster Computing*, vol. 21, no. 1, pp. 333–346, 2017.

[28] S. Latif, S. Mahfooz, B. Jan et al., "Multicriteria based next forwarder selection for data dissemination in vehicular ad hoc networks using analytical network process," *Mathematical Problems in Engineering*, vol. 2017, Article ID 4671892, 18 pages, 2017.

[29] W.-M. Wey and K.-Y. Wu, "Using ANP priorities with goal programming in resource allocation in transportation," *Mathematical and Computer Modelling*, vol. 46, no. 7-8, pp. 985–1000, 2007.

[30] T. L. Saaty, "Decision making with dependence and feedback: the analytic network process," in *An Integrated Approach for Machine Tool Selection Using Fuzzy Analytical Hierarchy Process and Grey Relational Analysis*, A. Samvedi, V. Jain, and F. T. S. Chan, Eds., vol. 50, article 32113221 of International Journal of Production Research, p. 1996, RWS Publications, Pittsburgh, PA, 2012.

[31] T. L. Saaty, *Theory and Applications of the Analytic Network Process: Decision Making with Benefits, Opportunities, Costs, and Risks*, RWS Publications, 2005.

[32] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," in *2008 IEEE International Conference on Communications*, pp. 2129–2133, Beijing, China, May 2008.

[33] K. A. Hafeez, L. Zhao, Z. Liao, and B. N.-W. Ma, "Impact of mobility on VANETs' safety applications," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–5, Miami, FL, USA, December 2010.

[34] O. Abedi, M. Fathy, and J. Taghiloo, "Enhancing AODV routing protocol using mobility parameters in VANET," in *2008 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 229–235, Doha, Qatar, March-April 2008.