IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 27, 2017, accepted July 19, 2017, date of publication July 28, 2017, date of current version August 22, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2733225

A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing

SEYED AHMAD SOLEYMANI[1], ABDUL HANAN ABDULLAH[1], (Member, IEEE), MAHDI ZAREEI[2], (Member, IEEE), MOHAMMAD HOSSEIN ANISI[3], (Member, IEEE), CESAR VARGAS-ROSALES[2], (Senior Member, IEEE), MUHAMMAD KHURRAM KHAN[4], (Senior Member, IEEE), AND SHIDROKH GOUDARZI[1]

[1]Universiti Teknologi Malaysia, Johor Baharu 81310, Malaysia
[2]Instituto Tecnologico y de Estudios Superiores de Monterrey, Monterrey 64849, Mexico
[3]School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, U.K.
[4]King Saud University, Riyadh 11653, Saudi Arabia

Corresponding author: Mohammad Hossein Anisi (anisi@ieee.org; anisii@gmail.com)

This work was supported by the Research Focus Group on Telecommunications and Networks of the Escuela de Ingeniería y Ciencias at Tecnologico de Monterrey, and by the basic science SEP-CONACYT Project under Grant CB-2015-01-0255387.

ABSTRACT In vehicular ad hoc networks (VANETs), trust establishment among vehicles is important to secure integrity and reliability of applications. In general, trust and reliability help vehicles to collect correct and credible information from surrounding vehicles. On top of that, a secure trust model can deal with uncertainties and risk taking from unreliable information in vehicular environments. However, inaccurate, incomplete, and imprecise information collected by vehicles as well as movable/immovable obstacles have interrupting effects on VANET. In this paper, a fuzzy trust model based on experience and plausibility is proposed to secure the vehicular network. The proposed trust model executes a series of security checks to ensure the correctness of the information received from authorized vehicles. Moreover, fog nodes are adopted as a facility to evaluate the level of accuracy of event's location. The analyses show that the proposed solution not only detects malicious attackers and faulty nodes, but also overcomes the uncertainty and imprecision of data in vehicular networks in both line of sight and non-line of sight environments .

INDEX TERMS Trust, plausibility, experience, fog node, fuzzy logic, VANET.

I. INTRODUCTION

Vehicular Ad hoc NETwork (VANET) is a method to increase the safety of roads. VANET is commonly obtainable through communications either between two vehicles (V2V), or between a vehicle and an infrastructure (V2I). Vehicles can broadcast warning messages and traffic management instructions in the vehicular environment to raise driver's awareness of possible travel hazards. In terms of comfort and convenience of passengers, vehicles can also exchange, for example, multimedia with other vehicles in the network. Since the number of accidents and unsatisfied users in vehicular networks are considerably increasing; currently, the main concern in this field is to enhance the road safety and ensure passenger comfort, which are achievable by intelligent transportation systems. Although many technical efforts have been carried out to achieve the goals of VANET, it still exhibits several downsides. For instance, since the mobility of vehicles is relatively high, it burdens on the service constrained communications and leads to a high cost communication. Due to the unique features of the vehicular environment, the applied technologies as well as the suitable security model have the vital role to enhance the safety of the passengers. From technology vantage point, Cisco (2012) developed Fog Computing (FC) as a paradigm that broadens cloud computing and services to the edge of the network instead of entirely in the cloud. In addition, fog computing is a promising method for to fulfil VANETs requirements. For example, fog computing offers a quick reaction to underlying device. It also reduces the burden on the cloud and offers the ability to analyse the data stream real-time with the cloud, [1].

According to [1], fog computing is a suitable method to increase the safety services and improve traffic management which both require local information and real-time processing. Due to the advantages of edge location, fog computing

has ability to support applications with low latency requirements, [2]. Hence, in this work, fog computing is adopted as a reliable storage of local information of the vehicular environment.

In terms of a security model, since the data and event messages are bases of the vehicular environment, hence integrity and accuracy of data, and the negative impact of inaccurate data on network performance, as well as trustworthiness among vehicles are interesting issues. It is obvious that presence of attacks, as security threats [3], reduces data accuracy leading to a lower network efficiency. Various security risks and attacks have been introduced including physical attacks on network devices and communication attacks, such as message forging, message tampering, reply attacks, wormhole attacks, and privacy invasion. Obstacles, such as buildings and trucks moving on the road, can also be considered as types of threats that can influence localization service integrity, reliability, and availability [4]. These objects can block a driver's visual and communication line of sight (LOS) by making a non-line of sight (NLOS) state.

During the past decade, many solutions have been introduced to overcome the existing security threats in vehicular network, [5]. However, since in VANET the mobility of the network vehicles is significantly high and the number of network entities are extremely large, faulty nodes, malicious attackers and obstacles are still huge security challenges. Moreover, because of the characteristics of VANET, the network information of the vehicular environment known by each node is inaccurate, incomplete, and imprecise. With respect to the significance of data in the vehicular network, it is clear that, uncertainty of data has negative impact on drivers' behaviour and it threatens the security of VANET as well.

Based on the problems evaluation, we are motivated to propose a trust model using fog computing that not only detects malicious attackers and faulty nodes, but also tackles the uncertainty and imprecision of data in the vehicular network in both LOS and NLOS states. Based on the proposed model, each vehicle individually measures the trust level of the sender of an event message by performing fuzzy logic. First the proposed model measures the plausibility and experience level of the sender. Next, it extracts the position of received event message using the relevant data stored in the closest fog nodes. Based on the extracted data, it subsequently measures the level of accuracy of the event message using fuzzy logic. Finally, a decision-making module decides on the sender of the event message. The receiver accepts and relays on the event message if the sender is trustable, denies it otherwise.

The rest of this work is organized as follows: Section 2 provides an overview of related works. Section 3 shows the attacks and security requirements. Section 4 presents the proposed model and the designed fuzzy inference system. Performance evaluation is described in Section 5. Finally, Section 6 concludes the work.

II. RELATED WORK

Dealing with the problems caused by the attacks (such as physical and communication attacks) as well as immovable/movable obstacles in the vehicular area are thorny issues for safety engineers. Since each network has its own features and requirements, numerous security frameworks and solutions have been proposed. In this study, to improve safety of the vehicular environment, we focus on both trust and plausibility as two elements of the security solution. Therefore, we look at related work in these areas, separately.

A. PLAUSIBILITY MODEL

Plausibility, as a part of a security system, verifies the information relevant to an event [5]. It has also been introduced as a mechanism to ensure positional reliability. According to [6] data plausibility checking is also utilized to evaluate trustworthiness of vehicles.

To check the plausibility of mobility data of single-hop neighbour nodes, a specific filter algorithm was adopted in [6]. The algorithm executes a data fusion of several location-related data sources. To increase quality of performance of checking, they utilized different independent information sources that confirm or reject a particular situation. A similar approach based on Kalman filter has been also presented in [6] to track surrounding nodes and identify variations in their mobility behaviour.

Lo *et al.* [7] introduced a new type of attack, which produces an illusion to its surrounding vehicles using broadcasts of the scene-aligned traffic warning messages. To eliminate this security attack, they have developed a model based on plausibility. For this purpose, they defined a set of five rules. Depending on the given rule set, if a message passes all validation processes constructed by these rules, it is accepted, otherwise it is discarded. However, this model, like other proposed models, is only limited to detect illusion attacks. In addition, with respect to the uncertainty information in vehicular network, it seems that passing all rules in order to accept the message is too strict.

To identify and exclude security attackers, a central scheme has also been proposed in [8]. The proposed scheme, based on trust and reputation information, focused on Sybil attack which was capable of forging messages to generate ghost vehicles. However, due to the unique features of VANET such as high mobility of vehicles and large scale of network, centralized schemes are not suitable in vehicular environments. Moreover, this model is only able to eliminate the Sybil attacks.

B. TRUST MODEL

Trust, as an element of security [9], has a vital role to cope with attacks in the vehicular network, [4]. A comprehensive and systematic review of existing trust models is proposed in our previous research, [10]. In this survey, first we categorized the trust models into three groups, and later we compared the proposed models based on

six metrics. We also described the advantages and disadvantages of proposed models.

To eliminate inconsiderate vehicles from the network, which usually attempts to increase the utility of car owners to the fullest by sending out false information, Minhas *et al.* [11] proposed a framework to model the reliability of the agents of adjacent vehicles. The entity-trust model was considered as a multi-layered trust modelling approach that takes role, experience, priority and majority-based trust into account. In [12] an infrastructure-based trust model has been proposed to identify malicious or inconsiderate nodes propagating false or fake information. The model exhibited a promising performance with relatively high speed and precision since the reputation was scored by recommendations given by other vehicles and road-side infrastructure units (RSUs). In the model, fuzzy logic and probability have been used in order to make the decision. To calculate trust value by entity-centric trust models, adequate information about the neighbours and sender of message is required. However, since the mobility of vehicles is considerably high, the model has failed to harvest sufficient information about the adjacent vehicles or other senders.

Raya *et al.* [13] extensively discussed that vehicles might become fake or their reliabilities become partially or fully compromised by attackers, which require their reliabilities to be revoked. They proposed a data-centric trust model that computes trust in each individual piece of data. However, the model suffers from prolonged latency and data loss since the trust model requires measuring the trustworthiness of received event messages one by one, and the data might be duplicated which causes a heavy traffic density in the network. Yao *et al.* [14] also proposed a dynamic entity-centric trust model to obtain reliable data and make the applications work efficiently. To identify malicious nodes and their strategies in a real-time scenario, a trust model is proposed for VANETs using a robust algorithm in [15]. The proposed model follows game theoretic approach implementing Nash equilibrium to calculate best strategy for attacker and defender through a payoff matrix. It verifies the information and messages to identify trusted nodes for reliable communication.

To the best of our knowledge, none of the above methods have focused on NLOS to measure the trust factor, while immovable obstacles on the sides of the road (e.g. buildings, trees, and area topography) and moving obstructions (e.g. trucks) interfere radio signals and prevent a desirable communication. Hence, obstacles can influence the integrity, reliability and availability of the event message.

III. ATTACK AND SECURITY REQUIREMENTS

In order to design and evaluate a new security model, three processes namely identifying threats, challenges and requirements are required, [4]. In this section, we define security requirements as well as possible attacking scenarios in vehicular networks.

A. ATTACK AND SECURITY THREATS

In this article, it is assumed that the following attacking scenarios are possible:

- **Bogus Message:** The goal behind this kind of attack is to send wrong information in the network.
- **Message Alteration:** It occurs when erroneous information is provided or when information that passes through a node is modified, [16]. The involved requirement in this attack is integrity of message.
- **Obstacles:** Movable/immovable obstacles, as security threats, can form a case of NLOS, which will interrupt direct communication among vehicles and prevent vehicles from properly checking their neighbouring nodes, [17].

B. SECURITY REQUIREMENTS

The aim of this work is to design a scheme for the provision of a secure environment in VANET. A system for securely messaging in a VANET needs to fulfil the following requirements:

- **Authentication:** Vehicle responses to any events should be based on validated messages. Hence, first, the senders of the messages are required to be authenticated, [18].
- **Message Integrity:** The integrity of the message should be examined since the message might be changed between the sending and receiving moment, and it must be completely matched to what it is sent. In a broader sense, the validity of the message also includes its consistency with similar one. That is to say, those messages that are generated in a closer space and time are more reliable. It should be noted that the sender might be legitimate, while the message contains fabricated data.
- **Confidentiality:** Application scenario determines the message confidentiality in VANET. Confidentiality is achievable by adopting public or symmetric key encryptions to assure the security of the communications, [19].
- **Location Validation:** It identifies that whether the provided location of an adjacent node is real or fake.
- **Availability:** The availability of node is required to be supported by alternatives means since even in a robust communication channel, some tricky attacks are able to jam the network such as DoS. That is, in the presence malicious nodes the network should be operational.

IV. PROPOSED MODEL

The proposed trust model accesses the accuracy and integrity of a sender of the event message by performing fuzzy logic. To this end, upon receiving an event message from surrounding vehicles, first it checks the authentication of the sender using authentication module. It uses ID authentication to evaluate the sender of the event message whether it is authorized or not. Simultaneously, it checks the lifetime of the event message calculating the difference between the generation time of the message included in the event message

and the current time. By performing fuzzy logic, it extracts the accuracy level of the location of the event included in the message if it exists in the closest fog nodes afterwards. Next, it evaluates the trust value based on experience, plausibility, and accuracy level of location, where experience and plausibility are dependent upon past direct interaction and location verification using distance and time, respectively. Finally, based on severity level of trust value, the decision-making module decides on event message whether it is acceptable or not.

Since the fuzzy logic is the main approach adopting in this work, a short description of the method and underlying reasons for adopting this approach are presented in the following section. Each module will be explained and discussed in detail subsequently.

Why Fuzzy Logic? Unlike classical theories, in the fuzzy theory, each elements can have a level of membership. The fuzzy set theory is also able to reflect vague and inadequate information by a defined set membership as a potential distribution. Moreover, it relies on the concept of approximation rather than precise determinations. The fuzzy logic is increasingly being adopted in several applications in many industries due to its capabilities to deal with approximation reasoning. In addition, it is simple to grasp conceptually, tolerant of data imprecision, and flexible, which is inspired from a natural language. Inaccuracy, incompleteness, and imprecision of the network information sent by each node indicate that we can use the fuzzy logic theory in vehicle environment since it is a promising artificial intelligence technique with reliable performance in the decision-making systems. Since the large number of terms used for describing, radio signals are fuzzy in nature [20] and because of the inherent strength of fuzzy logic to tackle uncertainty and imprecision, the fuzzy logic is adopted in this work.

A. AUTHENTICATION MODULE

In the proposed model, we consider a module to assess authentication of a sender as the first and main requirement for any security system. Certain data associated to the transmitting node are extremely essential in VANET. Such data can be identification information of the senders in addition to their features and locations. It is also imperative to authenticate all events, in which users are communicating or data is being exchanged throughout the network. The level of authorization of vehicles is monitored by authentication, which protect the VANET from Sybil attacks by giving a certain identity to each vehicle. As a particular example, a car might claim that it is a set of vehicles, which creates an illusion that there is a congested road. Congestion avoidance can handle this fake information and prevents the illusion. External methods can be used by power authentications to provide real and reliable evidence in order to detect attacks. Such externals methods can be traditional law enforcement authorities. Kargl *et al.* [21] mentioned that authentication ensures that the sender of a message is correctly identified. They introduced ID authentication, property authentication, and location authentication to verify ID of sender, properties of the sender, and the claimed position by sender, respectively.

In the proposed scheme, we use ID authentication to evaluate the sender of event message whether it is authorized or not. ID authentication gives a vehicle the ability to identify the transmitter of a message in an exclusive way. This authentication also allows a vehicle to be part of the network. Once the ID authentication is executed avoiding specific attacks, such as impersonation and fake nodes, will be simple tasks. Therefore, the digital certificates proposed by the IEEE 1609.2 standard [22] is adopted in this work. In this standard, the security service is based on elliptic curve cryptography (ECC), public key certificates and the public key infrastructure (PKI).

B. LIFETIME CHECKING

Due to the high mobility of vehicles and consequently high dynamic behaviour, the lifetime of the message is an important issue in VANET. In other words, fresh messages are more reliable than old/expired messages in the vehicular environment. Note that the lifetime is the time interval between the event time and the expiration time of the event message. To deal with old/expired messages as redundant messages, the proposed system first checks the lifetime of the event message. Hence, the system calculates the difference between the event time ($Time_E$), which is included in the message, and the current time ($Time_{current}$). Furthermore, depending on the type of event message and current condition of vehicular environment, the threshold time for the event message ($Time_{threshold}$) will be evaluated. For example, it should be set at a large value under sparse traffic scenarios or small under dense traffic situations. If the event message is too old/expired, it will be discarded. Otherwise, it will be sent to the next step to further bechecked (see Algorithm 1).

Algorithm 1 Lifetime Checking

Input (Msg, $Time_{current}$, $Type_{event}$)
$Time_{diff}$ = **Calculate-Diffrence**($Time_{current}$,$Time_E$)
$Time_{threshold}$ = **Extract-Threshold-Time** ($Type_{event}$)
if $Time_{diff} > Time_{threshold}$ **Then**
    Discard Event message
else
    Go to next step

C. EXPERIENCE MEASUREMENT MODULE

In this section, we develop a module to measure experience by performing fuzzy logic. Based on this module, each vehicle individually measures the level of experience of the sender of the event message. According to [11], the experience of direct interactions between nodes can be a factor to determine the level of trust. To be more precise, the history of past interactions between nodes is effective to update one node's belief in the trustworthiness of another. It is obvious that nodes with good history of past interactions have positive

impact on the trust score. On the contrary, bad experience in past interactions decreases the level of trust. Therefore, it is essential that each node in the VANET stores the history of preceding interactions with others node. The stored information can be used to evaluate the trust-worthiness level of the nodes based on their previous experiences afterwards.

Building on this, we propose a module to compute the level of trust of the sender based on experience. Our experience-based trust represents a factor of trust that is based on direct interactions. In addition, the proposed experience-based trust is monitored for each particular node in the system which is regularly updated depending on the requested vehicle's satisfaction with the given advice once it is asked. The proposed experience-based trust model is also accumulative so that it repeatedly updates the level of node's trust. As a result, to make the system scalable, the system requires only the storing of the most recent trust values and the number of interactions between nodes. In this work, the computation of the trust is formalized.

The range of values of all personal experience-based trust can be set either to 0 or 1, where 1 is indicative of absolute trust and 0 represents utter distrust. Thus, the following procedures can be executed to update the value of a node's personal experience trust, which has been previously done in [23].

Let $EXP_V(W) \in (0, 1)$ be the value indicating the extent to which V trusts (or distrusts) node W according to V's personal experience in interacting with W. After V follows an advice of W, if the advice is evaluated as reliable, then depending on the level of current value of experience (Low, Medium and High), the trust value $EXP_V(W)$ is increased by Algorithm 2, where $0 < \alpha < 1$ is a positive increment factor. Otherwise, if W's advice is evaluated as unreliable, then $EXP_V(W)$ is decreased by Algorithm 3, where $-1 < \beta < 0$ is a negative decrement factor and Min_l, Min_m, Min_h are 0, 0.3 and 0.6, respectively.

Algorithm 2 Experience Measurement When Sender Advice Evaluated as Reliable

if $EXP_{current}$ is Low **then**
  $EXP_{new} = (EXP_{current} - Min_l) + Min_m$
if $EXP_{current}$ is Medium **Then**
  $EXP_{new} = (EXP_{current} - Min_m) + Min_h$
if $EXP_{current}$ is High **then**
  $EXP_{new} = EXP_{current} + \alpha\,(1 - EXP_{current})$
if $EXP_{new} > 1$ **then**
  $EXP_{new} = 1$

Due to the dynamic environment the absolute values of α and β depend on other factors such as the event/task-specific property and the data sparsity situation. For instance, in the case that the interaction data is small, these values required to be set to its maximum allowing more weights to the available data. For more serious events such as collision avoidance, $|\alpha|$ and $|\beta|$ should be larger, to allow the system to reduce or increase the values of trust of reporting agents faster. It should also be noted that we might set $|\beta| > |\alpha|$ by having $|\beta| = \mu\,|\alpha|$ and $\mu > 1$ to facilitate the common assumption that building up a trust should be strenuous, but easily susceptible to be torn down. Setting too generously possibly results in being too trusting of certain agents. Lenient values for α leads the system to be over trusting of certain agents. On the other hand, setting β austerely will result in decreasing the number of agents being trusted. Of course, under some specific conditions the system is required to be strict and very defensive but it is not always the case. Based on the conditions and situations, we should learn through experience that which values are the best for a particular case.

Algorithm 3 Experience Measurement When Sender Advice Evaluated as Unreliable

if $EXP_{current}$ is High **then**
  $EXP_{new} = (EXP_{current} - Min_h) + Min_m$
if $EXP_{current}$ is Medium **Then**
  $EXP_{new} = (EXP_{current} - Min_m) + Min_l$
if $EXP_{current}$ is Low **then**
  $EXP_{new} = EXP_{current} + \beta\,(1 - EXP_{current})$
if $EXP_{new} < 0$ **then**
  $EXP_{new} = 0$

It is also worthy to note that formulas of the experience-based module are valuable to deal with nodes who attempt to build up trust and deceive afterwards. Under this condition, trust must be torn down immediately once deception is detected. Penalizing dishonest agents harshly discourage and acts as a deterrent and prevent them from simply gathering information from other nodes in order to boost their trustworthiness. Since it is possible this information may be inaccurate, this strategy runs the risk of severely destroying trustworthiness.

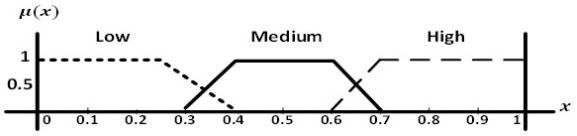

FIGURE 1. Experience level (EL).

As mentioned earlier, the proposed experiment measurement module is based on fuzzy logic. In this approach, fuzzification is the first step to adopt fuzzy logic technique to a real application. In this step, classical data or crisp data convert into fuzzy data or membership function. Therefore, the measured experiment value, as crisp data, is the input parameter to be fuzzified, as illustrated in Fig. 1. The membership functions named Low, Medium and High are used to represent the Experience Level(EL). The selection of EL membership functions can be derived based on experience as well as trial and error of the application requirement. As stated above, the range begins at 0 and ends to 1.

D. PLAUSIBILITY MODULE

In this module, plausibility of sender will be evaluated based on location verification of sender. This is because the

location verification enables vehicles to verify received location information and validate its integrity [24]. Shaikh *et al.* [25] also mentioned that location verification is used to determine the correctness of the location information.

In this study, the proposed scheme evaluates the correctness of sender's location using two modules including Location Verification Using Distance (LVoD), and Location Verification Using Time (LVoT) under both LOS and NLOS condition. The output of this algorithm is the plausibility level of sender ($PLAUS_{Level}$), as shown in Algorithm 4.

Algorithm 4 Evaluate the Plausibility Level of Sender

Input (Msg)
LVoD = **Location Verification of SENDER** (Distance)
LVoT = **Location Verification of SENDER(Time)**
$PLAUS_{Level}$ = **Fuzzy-DM** (fuzzify(LVoD),fuzzify(LVoT))
Output ($PLAUS_{Level}$)

1) LOCATION VERIFICATION USING DISTANCE(LVOD)

In this study, location/position verification is the most important factor to check plausibility of sender. It determines whether the sender has provided its true location or not. Distance measurement between sender and receiver is a way to verify a claimed position. Building on this, our proposed scheme calculates the distance between two vehicles using both GPS location information (X, Y) in a two dimensional plane ($Distance_{GPS}$) and radio signal strength (RSS) computation ($Distance_{RSS}$). This is because the implementation of RSS to estimate distance is simpler with lower cost compared to other radio range measurement techniques such as Time of Arrival, Angle of Arrival, and Time Difference of Arrival [26].

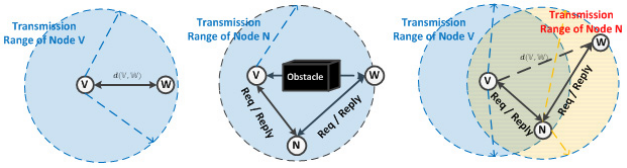

FIGURE 2. (a) Direct communication, (b) Indirect communication because of the obstacle, (c) transmission range limitation.

Under LOS condition, where there are no obstacles between transmitter and receiver (see Fig. 2.a), the proposed scheme measures $Distance_{GPS}$ between receiver (V) and sender (W) using Eq.1. In addition, node V calculates $Distance_{RSS}$ to node W by measuring the RSS which we are presenting next.

$$Distance_{GPS} = \sqrt{|X_V - X_W|^2 + |Y_V - Y_W|^2} \tag{1}$$

where (X_V, Y_V) and (X_W, Y_W) are the coordinates of sender and receiver, respectively.

Under NLOS condition, because of the immovable/movable obstacles as well as limitation of transmission range (see Fig. 2.b and 2.c), receiver (V)measures distance from sender (W) using a request that it will broadcast to its direct neighbours (e.g. node N). It is important to notice that in this situation, node V tries to send a request to its direct neighbours who have the good experience in the past communication. Upon reception a verifying location message about node W through its direct neighbours (N), node V calculates $Distance_{GPS}$ to W new coordinates of sender and receiver's location using Eq.1. It is obvious that a change in the coordinates of nodes is because of the mobility in VANET.

In addition, node V computes the $Distance_{RSS}$ to node W through node N by

$$Distance_{RSS} = \sqrt{(d_{VN})^2 + (d_{NW})^2 - 2d_{VN} \cdot d_{NW} \cdot cos\theta} \tag{2}$$

where d_{VN} is distance between V and W and d_{NW} is distance between N and W that measured using the RSS. The θ is the angle between vectors $\vec{U}$ and $\vec{Z}$ that are calculated by

$$\theta = ArcCos(\frac{\vec{U} \cdot \vec{V}}{\left\|\vec{U}\right\| \cdot \left\|\vec{V}\right\|}) \tag{3}$$

where $\vec{U} = \vec{NV} = (U_1, U_2) = ((X_V - X_N), (Y_V - Y_N))$ and $\vec{Z} = \vec{NW} = (Z_1, Z_2) = ((X_w - X_N), (Y_W - Y_N))$. In addition, $\vec{U}.\vec{Z} = U_1.Z_1 + U_2.Z_2$ and $\left\|\vec{U}\right\| = \sqrt{U_1^2 + U_2^2}$ and $\left\|\vec{Z}\right\| = \sqrt{Z_1^2 + Z_2^2}$.

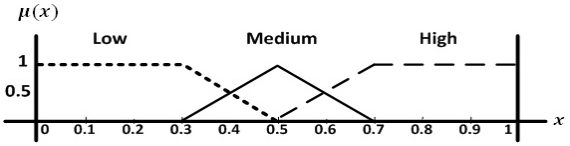

FIGURE 3. Difference distance level.

In order to verify sender, the proposed scheme computes $Dist_{diff} = |Distance_{RSS} - Distance_{GPS}|$ and then evaluates the severity level of $Dist_{diff}$ by converting this value to fuzzy data. We consider $Dist_{diff}$ having a certain severity level. As shown in Fig. 3, for the purpose of simplicity, we will take three fuzzy sets into account as Low, Medium and High to represent the LVoD. The selection of LVoD membership functions are determined according to experience as well as trial and error of the application requirement, hence the range is between 0 and 1.

Distance Measurement Using RSS: As mentioned above, under both LOS/NLOS condition, receiver has to calculate its distance ($Distance_{RSS}$) from sender by measuring the RSS. However, due to the path loss exponent uncertainties, inaccuracy is the most important weakness in RSS-based distance measurement [26]. Therefore, in a non-free space area such as in vehicular networks, using RSS for distance estimation, as it is seen in Eq.4, without knowing the path loss exponent is not possible. This is because the path loss exponent will be changed due to changing environment.

$$RSSI_{ij} = (10\gamma \cdot log_{10}Distance_{ij} + X) \tag{4}$$

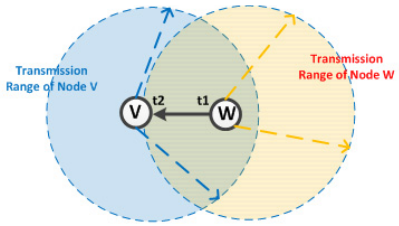

FIGURE 4. Direct communication.

where γ is the path loss exponent, $Distance_{ij}$ represents distance between node i and node j, X is the received signal strength at 1 meter distance. Due to the importance of path loss exponent to estimate distance using RSSI, we use the proposed approach for dynamic estimation of path loss exponent presented in [26].

2) LOCATION VERIFICATION USING TIME (LVOT)

Time verification is another way to detect a falsely claimed position [27]. To this end, assuming that both location information of the sender and receiver are correct, the expected received time of the message will be calculated. According to [25], the value of this time depends on the distance between two vehicles and propagation speed. Based on the physical medium of the link, propagation speed is between $2\times10^8(m/s)$ and $3\times10^8(m/s)$, [28]. In this study, we assumed that the speed of signal propagation is equal to the speed of light, $c = 3 \times 10^8$.

Under LOS condition where sender and receiver have direct communication, we suppose that node W sends a message to V at t_1 and node V received the message at $time_{rec}$ (see Fig. 4). It is expected that node V received the message at $time_{exp}$ that is measured using the following, [27], [29]:

$$time_{exp} = t_1 + \frac{Dist(V_{t_2}, W_{t_1})}{c} \tag{5}$$

where $Dist$ is distance between receiver and sender calculated by Eq.1 and $c = 3 \times 10^8$.

Under NLOS condition, to verify node W, node V not only calculates $time_{exp}$ by Eq.6 but also it sends a request to its direct neighbours who has direct communication with W (e.g. node N). Then, node N sends a request to W and waits to reply. Upon receiving the response from W, node N immediately measures $time_{exp}$ using Eq.5 and checks the validity of W by comparing the expected and received times as mentioned earlier. Node N then will send back a reply to, if node W is valid.

In order to check the validity of a sender, the proposed scheme computes $Time_{diff} = |time_{exp} - time_{rec}|$ and then evaluates the severity level of $Time_{diff}$ by converting this value as crisp value to fuzzy data. Like previous section, two fuzzy membership named Acceptable and Not-Acceptable are considered to represent LVoT. Node V verifies node W if this value is placed in the acceptable level, otherwise it is not confirmed. As illustrated in Fig. 5, the range is between 0 and 1.

Fuzzy inference process is the second step to implement fuzzy logic. This step combines the membership functions

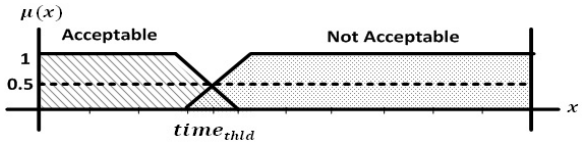

FIGURE 5. Difference time level.

TABLE 1. Fuzzy inference engine to determine plausibility level.

Rule No.	LVoD	LVoT	Plausibility Level (PL)
1	High	Acceptable	High
2	High	Not-Acceptable	Medium
3	Medium	Acceptable	Medium
4	Medium	Not-Acceptable	Low
5	Low	Acceptable	Medium
6	Low	Not-Acceptable	Low

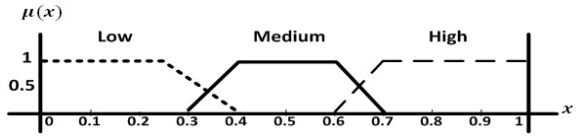

FIGURE 6. Plausibility level (PL).

with the control rules to derive the fuzzy output. The fuzzy inference engine is a developed group of rules using expert knowledge. In order to evaluate the certain level of plausibility, we design the knowledge-based rules that links the inputs and the outputs. These rules are associated to a careful understanding of the philosophy behind vehicular network behaviour. As presented in Table 1, the fuzzy inference engine to determine plausibility level is based on 6 rules. As illustrated in Fig. 6, the membership functions named as Low, Medium, and High are used to presented the PL. The selection of PL membership functions is based on trial and error of the application requirements and its range is between 0 and 1.

E. ACCURACY LEVEL MEASUREMENT USING FOG NODE

Despite the increasing usage of cloud computing, there are still unsolved issues due to the inherent problem of cloud computing such as unreliable latency, lack of mobility support, and location-awareness. Fog computing, also named edge computing, can address those problems by providing elastic resources and services to end users at the edge of network, while cloud computing is more about providing resources distributed in the core network [30]. According to [31], fog computing has emerged as a promising technology that can bring the cloud applications closer to the physical IoT devices at the network edge.

In fog computing, facilities or infrastructures that can provide resources for services at the edge of the network are called fog nodes. It is the physical device where fog computing is deployed [31]. They can be resource-poor devices such as set-top-boxes, access points, routers, switches, base stations, and end devices.

In this paper, we assumed that fog nodes in vehicular environment store all relevant data on events that occurred

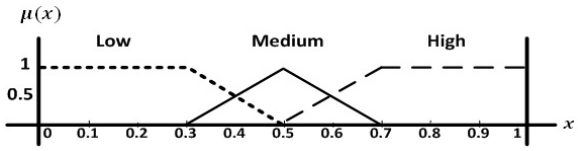

FIGURE 7. Accuracy level based on difference distance (AL).

in their area. The stored data can include the location and the time of event. Building on this, we propose a module to measures the accuracy level of location of event using fuzzy logic. This module attempts to send a request to closest fog nodes about the event's location. If a fog node $FoGN_i$ receives the request, it will first verify the request by checking the existence of event in its event list. If it exists, it replies to sender the relevant information of event, immediately. Upon reception of a verifying message from one of the fog nodes ($FoGN_i$), it calculates the difference between location sent by fog node and location included in message using

$$Distance_{fgn-msg} = \sqrt{(x_{fgn} - x_{msg})^2 + (y_{fgn} - y_{msg})^2} \quad (6)$$

where (x_{msg}, y_{msg}) and (x_{fgn}, y_{fgn}) are the event location coordinates included in the message and sent by fog node, respectively.

We consider $Distance_{fgn-msg}$ having a certain severity level. As shown in Fig. 7, for the purpose of simplicity, we will take three fuzzy sets into account as Low, Medium, and High to represent the AL. The selection of AL membership functions is based on experience as well as trial and error of the application requirement, thus the range begins at 0 and ends to 1.

F. DECISION MAKING MODULE

In the fuzzy logic, the fuzzifier transforms the input values into degrees of matching with linguistic values. In the proposed model, input parameters collected by the source vehicle are fuzzified using the predefined input membership functions shown in Fig. 4, 6 and 8. The fuzzification transforms the input value to names and degrees of membership in the functions.

After the fuzzification step of the input values, fuzzified generated values are used to evaluate the rules to obtain the trust level of a sender ($TRuST_{level}$). The fuzzy rule-base contains a number of fuzzy IFTHEN rules.

In our model, there are three input parameters including PL, EL, and AL. The input parameters are each composed of three fuzzy sets (Low, Medium and High). Based on the parameters we design the rule table including twenty-seven (27) IF-THEN rules to define the trust-level after the fuzzification step. The number of rules (N) depends on the number of input parameters and the number of fuzzy sets associated with the input parameter. The maximum possible number of rules is:

$$N = \prod_{i=1}^{NI} NFSI_i = 3 \times 3 \times 3 = 27 \quad (7)$$

TABLE 2. Fuzzy inference engine to determine trust level when fog node is available.

Rule No.	EL	PL	AL	$TRuST_{level}$
1	Low	Low	Low	Not-Acceptable
2	Low	Low	Medium	Not-Acceptable
3	Low	Low	High	Not-Acceptable
4	Low	Medium	Low	Not-Acceptable
5	Low	Medium	Medium	Not-Acceptable
6	Low	Medium	High	Not-Acceptable
7	Low	High	Low	Acceptable
8	Low	High	Medium	Not-Acceptable
9	Low	High	High	Acceptable
10	Medium	Low	Low	Acceptable
11	Medium	Low	Medium	Not-Acceptable
12	Medium	Low	High	Not-Acceptable
13	Medium	Medium	Low	Acceptable
14	Medium	Medium	Medium	Not-Acceptable
15	Medium	Medium	High	Acceptable
16	Medium	High	Low	Acceptable
17	Medium	High	Medium	Acceptable
18	Medium	High	High	Acceptable
19	High	Low	Low	Acceptable
20	High	Low	Medium	Not-Acceptable
21	High	Low	High	Acceptable
22	High	Medium	Low	Acceptable
23	High	Medium	Medium	Acceptable
24	High	Medium	High	Acceptable
25	High	High	Low	Acceptable
26	High	High	Medium	Acceptable
27	High	High	High	Acceptable

TABLE 3. Fuzzy inference engine to determine trust level when fog node is not available.

Rule No.	EL	PL	AL	$TRuST_{level}$
1	Low	Low	-	Not-Acceptable
2	Low	Medium	-	Not-Acceptable
3	Low	High	-	Not-Acceptable
4	Medium	Low	-	Not-Acceptable
5	Medium	Medium	-	Acceptable
6	Medium	High	-	Acceptable
7	High	Low	-	Not-Acceptable
8	High	Medium	-	Acceptable
9	High	High	-	Acceptable

where NI is the number of inputs and $NFSI$ is the number of fuzzy set of inputs.

Table 2 shows the fuzzy inference engine to evaluate $TRuST_{level}$. Since the usage of fog nodes may not be available at any time anywhere, our proposed model evaluates the $TRuST_{level}$ without considering the accuracy level (AL) using the rules defined in Table 3.

The final step is defuzzification, which is used to determine the value of the $TRuST_{level}$. In our system model, we consider the centroid defuzzification technique. This method is also known as center of gravity or centre of defuzzification area. This is the most commonly used technique and is reasonably accurate. The centroid defuzzification technique is computed using the following:

$$TRuST_{level} = \frac{\int x_i \cdot \mu(x_i)}{\int \mu(x_i)} \quad (8)$$

where $TRuST_{level}$ is the defuzzified output (it is the membership degree of output), $\mu(x_i)$ and x_i are the aggregated

FIGURE 8. Map of Kuala Lumpur from Open Street Map database.

membership function and the fuzzy value, respectively. The only disadvantage of this method is that it is computationally difficult for complex membership functions. However, in our system, membership functions have a simple trapezoid shape.

V. PERFORMANCE EVALUATION

In this section, we present the simulation evaluation and discuss the simulation results. To evaluate the performance of the proposed beacon rate adoption, we have implemented the proposed algorithm in a network simulator (ns-2) with SUMO and MOVE traffic simulator tool for urban environment. The SUMO is a free implementation of such a simulator and supports car-following model. As shown in Fig. 8, the OSM file of Kuala Lumpur, from Open Street Map database is also utilized. We set the maximum speed of vehicles at 110 m/s. The simulation area is set at 2 $km \times 2$ km and the maximum node density on the simulation area is 500 nodes. According to [11], on the optimal data rate, we set channel bandwidth at 6 Mbps for this simulation.

In physical layer, two-ray ground reflection model is used as radio propagation model. In addition, transmission range of vehicles is set at 250 meter. In our simulation, we used the IEEE 802.11p to simulate the MAC layer. AODV also utilized as routing protocol. The traffic source of the simulation is Constant Bit Rate (CBR) with a value of 36 kbps, which is based on UDP packet generation traffic. The total simulation time is 100 seconds. All configurations are simulated with 30 different random seeds to achieve a reasonable statistical significance.

A. EXPERIMENTAL RESULTS

This section shows the explanation of the initial carried out experimentations in order to validate the accuracy of proposed model.

Fig. 9 depicts the correlation behaviour between input and output variables. The trend shows that the value of output trust level increases when the value of plausibility is between 0.6 to 1 as well as experience between 0 to 0.4. Moreover, we can see that the output increases when plausibility between 0.4 to 1 and experience between 0.4 to 1. Thus, our fuzzy inference system could increase trust level as plausibility and experience increase or vice versa.

In order to evaluate the proposed model, there are two main conclusions that can be extracted from analyzing such results. In two cases, we evaluate the model with fog nodes and without fog nodes in both LOS and NLOS environments.

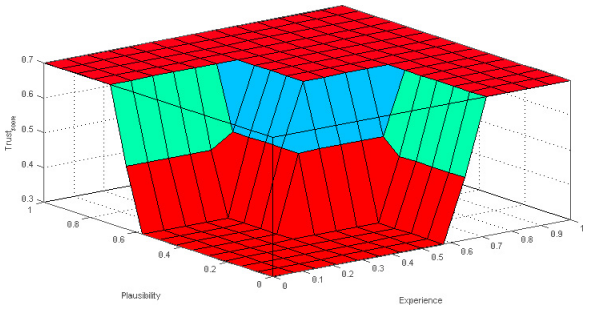

FIGURE 9. Correlation between inputs and output.

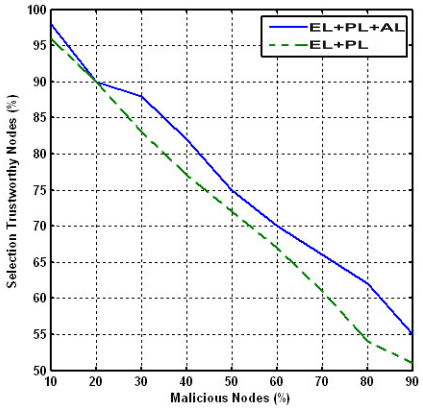

FIGURE 10. Accuracy evaluation without collusion.

First, in Fig. 10 we observe a detriment in the accuracy of the model as the percentage of malicious drivers increases. In the worst case, where 90% of vehicles in the VANET spread bogus or false traffic warnings, our model is capable to distinguish around 55% of the cases when the fog node is available. In the second test, when fog nodes are not available, our model is capable to fairly distinguish around 52%. In contrast, it is able to achieve an accuracy of around 98% and 95% with and without fog nodes where 10% of vehicles spread bogus traffic warnings. As shown in this figure, in the worst realistic scenario, when 50% of the users behave improperly, accuracy of our model is around 75%.

In the second experiment, malicious drivers collude in order to unfairly praise themselves while trying to decrease the reputation of actually benevolent ones. The results obtained after performing such experiments can be observed in Fig. 11. This figure shows that the trend of accuracy of our model is below 50% even using fog nodes (continuous line) and without using fog nodes (dashed line) where the percentage of attackers are greater than 80% and 85%, respectively. Again, in the worst realistic scenario (i.e. 50% of malicious drivers), our model is able to succeed around 73% of the times. According to [12], the trust model is not completely useless when the accuracy is below 50%.

As expected, the results of our evaluation show that the proposed model has better performance in terms of accuracy and integrity in comparison with TRIP [12]. In terms of com-

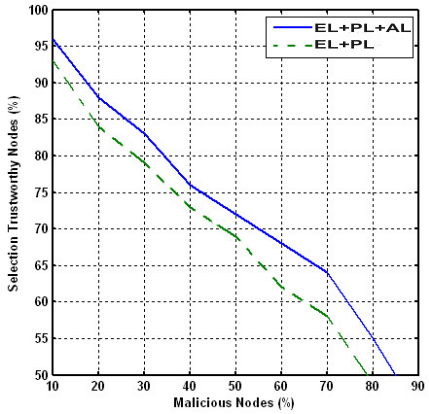

FIGURE 11. Accuracy evaluation with collusion.

plexity, because of the advances in chip manufacturing technology that have made it practical to embed fuzzy decision making systems in hardware chips, hence it ensures that the implementation of our model is simple.

VI. CONCLUSION

In this study, we show our proposal, as one of the useful solutions in order to usage trust management techniques in Vehicular ad hoc network. It is designed to be fast, light and accurate. Our simulation results clearly indicated that the proposed trust model performs a series of security checks to ensure the correctness of the information received from authorized vehicles. Actually, after surveying the current state of the art in this field, a number of design requirements for trust models in VANET are well defined. Some tests have proved the accuracy of our proposal under certain conditions. Moreover, we apply fog nodes as a facility to assess the level of accuracy of event's location. The simulation results show that our solution is not only able to detect malicious attackers and faulty nodes but also tackles the uncertainty and imprecision of data in vehicular network in both LOS and NLOS.

REFERENCES

[1] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, 2012, pp. 13–16.
[2] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular Ad-hoc networks: Paradigms, scenarios, and issues," *J. China Univ. Posts Telecommun.*, vol. 23, no. 2, pp. 56–96, 2016.
[3] J. M. De Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular Ad-hoc networks," in *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, M. Cruz-Cunha and F. Moreira, Eds. Hershey, PA, USA: IGI Global, 2011, pp. 894–911.
[4] S. Goudarzi *et al.*, "A systematic review of security in vehicular Ad Hoc network," in *Proc. 2nd Symp. WSCN*, 2013, pp. 1–10.
[5] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[6] N. Bismeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2012, pp. 78–85.
[7] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET applications—A message plausibility problem," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–8.
[8] N. Bismeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for vanets based on mobility data plausibility," in *Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl.*, 2012, pp. 73–82.
[9] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.
[10] S. A. Soleymani *et al.*, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 146, 2015.
[11] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011.
[12] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, 2012.
[13] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral Ad hoc networks," in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1238–1246.
[14] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017.
[15] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for Vehicular Ad hoc Networks (VANETs)," *Comput. Netw.*, vol. 121, pp. 152–172, Jul. 2017.
[16] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw.*, 2006, pp. 564–570.
[17] O. Abumansoor and A. Boukerche, "Towards a secure trust model for vehicular ad hoc networks services," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–5.
[18] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular Ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.
[19] V. S. Yadav, S. Misra, and M. Afaque, "Security in vehicular ad hoc networks," in *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Boca Raton, FL, USA, CRC Press, 2010, p. 227.
[20] G. El M. Zhioua, N. Tabbane, H. Labiod, and S. Tabbane, "A fuzzy multi-metric QoS-balancing gateway selection algorithm in a clustered VANET to LTE advanced hybrid cellular network," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 804–817, Feb. 2015.
[21] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for vanets," in *Proc. 4th Workshop Embedded Secur. Cars (ESCAR)*, 2006, pp. 1–10.
[22] IEEE "Draft standard for wireless access in vehicular environments—Security services for applications and management messages," Inst. Elect. Electron. Eng., Tech. Rep. 1609.2-20011 (D9), May 2011.
[23] T. Tran and R. Cohen, "A reliability modelling based strategy to avoid infinite harm from dishonest sellers in electronic marketplaces," *J. Bus. Technol.*, vol. 1, no. 1, pp. 69–76, 2005.
[24] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 275–285, Jan. 2012.
[25] R. A. Shaikh and A. S. Alzahrani, "Intrusion aware trust model for vehicular Ad hoc networks," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1652–1669, 2014.
[26] N. Alam, A. T. Balaie, and A. G. Dempster, "Dynamic path loss exponent and distance estimation in a vehicular network using doppler effect and received signal strength," in *Proc. IEEE 72nd Veh. Technol. Conf. Fall (VTC-Fall)*, Sep. 2010, pp. 1–5.
[27] S. Khan and J. L. Mauri, *Security for Multihop Wireless Networks*. Boca Raton, FL, USA: CRC Press, 2014.
[28] J. F. Kurose *Computer Networking: A Top-Down Approach Featuring the Internet*, 3rd ed. Reading, MA, USA: Addison Wesley, 2005.
[29] Z. Huang, "On reputation and data-centric misbehavior detection mechanisms for VANET," Ph.D. dissertation, Univ. Ottawa, Ottawa, ON, Canada, 2011.
[30] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data*, 2015, pp. 37–42.
[31] E. M. Tordera *et al.* (Nov. 2016). "What is a fog node a tutorial on current concepts towards a common definition." [Online]. Available: https://arxiv.org/abs/1611.09193

SEYED AHMAD SOLEYMANI received the B.S. degree from the Department of Computer Engineering, Sadjad University, Iran, and the M.S. degree from the Department of Computer Engineering, Islamic Azad University, Iran. He is currently pursuing the Ph.D. degree with the Department of Computing, Universiti Teknolgi Malaysia, Malaysia. His research interests are in wireless sensor network, mobile ad hoc network, vehicular ad hoc network, and visible light communication.

ABDUL HANAN ABDULLAH (M'15) received the Ph.D. degree from Aston University, Birmingham, U.K., in 1995. He was the Dean of the Faculty from 2004 to 2011. He is currently a Professor with the Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia. He is currently the Head of the Pervasive Computing Research Group, a research group under K-Economy Research Alliances. His current research interests include wireless sensor networks, vehicular ad-hoc networks, Internet of vehicles, network security, and next generation networks.

MAHDI ZAREEI (S'11–M'17) received the M.Sc. degree in computer network from the University of Science, Malaysia, in 2011, and the Ph.D. degree from the Communication Systems and Networks Research Group, Malaysia-Japan International Institute of Technology, University of Technology Malaysia, in 2016. He received JASSO Scholarship in 2015 to performed part of his Ph.D. research at Osaka University. He is currently a Post-Doctoral Fellow with the School of Engineering and Sciences, Tecnologico de Monterrey, Campus Monterrey. His research mainly focuses on cognitive radio network, wireless sensor network, ad hoc network, and optimization.

MOHAMMAD HOSSEIN ANISI (M'14) is currently a Lecturer with the School of Computer Science and Electronic Engineering, University of Essex, U.K. He received the Ph.D. degree from the Universiti Teknologi Malaysia. He was a Senior Lecturer with the Faculty of Computer Science and Information Technology, University of Malaya. He has also collaborated actively with researchers in several other disciplines of computer science. He has authored several papers in high quality journals and conferences. His research interests lie in the area of Internet of Things, wireless sensor networks and their applications, mobile ad hoc networks, and intelligent transportation systems. He is also an Active Member of the IEEE, the ACM, the International Association of Engineers, and the Institute of Research Engineers and Doctors. He received the Best Postgraduate Student Award. He is Associate Editor of the *Ad Hoc & Sensor Wireless Networks* (SCIE) and the *KSII Transactions on Internet and Information Systems* (SCIE) journals.

CESAR VARGAS-ROSALES (M'89–SM'01) received the M.Sc. degree in communications and signal processing and the Ph.D. degree in electrical engineering from Louisiana State University, Baton Rouge, USA. He was the Director of the Doctorate Program with the Information and Communications Technologies, Tecnologico de Monterrey, Campus Monterrey, from 2012 to 2016. He has co-authored the book *Position Location Techniques and Applications* (Academic Press/Elsevier). His research interests are personal communications, 5G, cognitive radio, MIMO systems, mobility, stochastic modeling, traffic modeling, intrusion/anomaly detection in networks, position location, interference, routing in reconfigurable networks, and optimum receiver design. He is a member of the Mexican National Researchers System (SNI), Level II, a member of the Academy of Engineering of Mexico, and a Regular Member of the Mexican Academy of Science (AMC). He is a Senior member of the IEEE Communications Society Monterrey Chapter Chair, and the Faculty Advisor of the IEEE-HKN Lambda-Rho Chapter. He was also the Technical Program Chair of the IEEE Wireless Communications and Networking Conference 2011.

MUHAMMAD KHURRAM KHAN (SM'12) is currently a Full Professor with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Kingdom of Saudi Arabia. He is one of the founding members of CoEIA and has served as the Research and Development Manager from 2009 to 2012. He developed and successfully managed the Research Program of CoEIA, which transformed the center as one of the best centers of research excellence in Saudi Arabia and in the region. He has authored over 250 research papers in the journals and conferences of international repute. He has invented ten U.S./PCT patents. He has edited seven books/proceedings published by Springer–Verlag and the IEEE. He has secured several national and international research grants in the domain of information security. He has played a leading role in developing the B.S. Cybersecurity Degree Program and the Higher Diploma in Cybersecurity at King Saud University. His research areas of interest are cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management.

SHIDROKH GOUDARZI received the master's and Ph.D. degrees from the Universiti Teknologi Malaysia in 2013 and 2017. Her field of study is communication system and wireless network. She has academic experience from Islamic Azad University, Iran. Her research interests are in wireless networks, artificial intelligence, and next generation networks.