Fuzzy Logic based Model for Energy Consumption Trust Estimation in Electric Vehicular Networks

Ilhem Souissi[1], Nadia Ben Azzouna[1], Tahar Berradia[2] and Lamjed Ben Said[1]

[1] *Strategies for Modelling and ARtificial inTelligence research Laboratory (SMART Lab), Institut Supérieur de Gestion de Tunis, Université de Tunis, Le Bardo, Tunis, Tunisia*

[2] *Institut de Recherche en Systèmes Électroniques Embarqués (IRSEEM Lab), ESIGELEC, Rouen, France*

Keywords: Trust, Energy Information, Attacks, Fuzzy Logic, Electric Vehicular Networks.

Abstract: Electric vehicles emerged new applications that are strongly related to the energy constraints such as the identification of the optimal path toward the vehicle's destination or toward the nearest recharging station, selection of the path where vehicle recovers extra energy, estimation of the need to recharge according to the actual battery state and the traffic state, etc. However, in electric vehicular networks, vehicles may provide wrong energy information due to sensors' failure, selfish or malicious reasons. Therefore, energy-related information trustworthiness needs to be evaluated in order to preserve the quality of the presented applications. In this paper, we address the energy-related information trustworthiness to discriminate between credible and erroneous values. Therefore, we propose a new fuzzy-based trust model that deals with the information uncertainties. This model aims at detecting the wrong energy information that mismatches with the vehicle's behavior and ensure that only trustworthy and plausible energy-information are handled. Results prove the performance of the proposed model and its capabilities to deal with several kinds of threats in different traffic densities with high precision.

1 INTRODUCTION

The Internet of Vehicles (IoV) is a typical application of the Internet of Things (IoT) in the transportation field. The main vision of the IoV is to enable multiple components to broadcast safety, efficiency and infotainment services (Alam et al., 2015). The IoV supports multiple kinds of communications such as Vehicle-to-Sensor (V2S), Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to-Human (V2H) (Sun et al., 2016). Similarly, the emergence of the Internet of Electric Vehicles (IoEV) involves the same kinds of communications. However, the IoEV also covers the Electric Vehicle-to-Electric Vehicle Supply Equipment communications (Bayram and Papapanagiotou, 2014). Over the last few years, Electric Vehicles (EVs) have emerged to meet with ecological issues mainly the environmental pollution and the lack of natural resources. These vehicles are cost-effective and easy to maintain (Bayram and Papapanagiotou, 2014) (Falk and Fries, 2012). However, EVs are energy-constrained and suffer from the limited battery capacity and the extensive charging time.

Alike the vehicular ad hoc networks (VANETs), the open, distributed and highly dynamic nature of the electric vehicular network makes it vulnerable to many security threats that may affect the quality of the provided services (Sumra et al., 2015). In such network, misbehaving entities may broadcast bogus and malicious information to affect the others' decisions. Hence, it is required to ensure the accuracy of the received data to make effective decisions and maintain the quality of services. Digital signature is usually dedicated to ensure authentication, integrity and non-repudiation (Al-Kahtani, 2012). However, this technique cannot prevent authenticated vehicles from misbehaving due to selfish reasons, malfunction of embedded sensors, etc. Consequently, it is required to assess the data trustworthiness so as to ensure that only reliable data are disseminated in the network.

In the past decade, several trust management solutions were proposed to overcome the security risks in VANETs (Soleymani et al., 2015) (Zhang, 2011). However, these solutions still present some limitations regarding the system's complexity, network security, etc. Moreover, sensed data in vehicular networks suffers from the fuzzy, inaccurate and uncertain nature due to the quality of embedded sensors, the intermittent connection, etc. Besides, to the best of

Souissi, I., Azzouna, N., Berradia, T. and Said, L.
Fuzzy Logic based Model for Energy Consumption Trust Estimation in Electric Vehicular Networks.
DOI: 10.5220/0006863202210233
In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT*, pages 221-233
ISBN: 978-989-758-319-3

our knowledge, none of the existing works addressed the trustworthiness of the energy-related information for EVs. Accordingly, in this paper we are interested in the accuracy of the energy-related information in electric vehicular networks. We are also interested in V2N communications that ensure a direct connection between vehicles and a central processing entity. Hence, we introduce a new fuzzy-based trust model to cope with the malicious threats that provide wrong energy information. This model considers two main dimensions; the instant energy verification and the total energy verification. On the one hand, the first dimension intends to filter the inaccurate energy information that mismatches with the vehicle's acceleration/ deceleration rate. On the other hand, the second dimension deals with the unsteady and uncertain behavior of EVs. In summary, the main contributions of this paper are:

- Propose a new fuzzy-based trust model in electric vehicular networks to evaluate the trustworthiness of the energy information based on two dimensions: the instant energy verification and the total energy verification.
- Provide a dynamic trust solution that adapts to the different traffic densities and road characteristics.
- Conduct experiments to validate the performance of the proposed solution to deal with multiple kinds of threats in different traffic densities.

The rest of the paper is organized as follows: Section 2 presents the related work. Section 3 provides an overview about the problem definition. Section 4 introduces the proposed trust model. Section 5 details the suggested fuzzy logic based model. Section 6 presents the simulation results and discussions and, section 7 concludes the paper.

2 RELATED WORK

In VANETs, multiple models for trust assessment are proposed to mitigate the security risks. These models are categorized into three main classes: the entity-centric trust, data/message-centric trust and hybrid trust (Zhang, 2011) (Soleymani et al., 2015).

In general, the entity-centric trust models stand on reputation and behavior evaluation. Reputation-based trust models integrate the previous experience, direct experience and recommendations from third parties. Usually, the reputation of an entity evolves over time according to its behavior. The more this entity behaves properly, the higher its reputation. Mármol and Pérez (Mármol and Pérez, 2012) assumed that the reputation score is computed according to previous interactions and recommendations from adjacent vehicles and from a central trusted authority. According to the computed reputation, the authors apply the fuzzy logic theory to decide whether to (1) reject the message, (2) accept the message but do not forward it, or (3) accept and forward the message. Wei et al. (Wei et al., 2014) also focued on reputation assessment. They adopted probability to evaluate the entity's reputation based on direct and indirect observations. Soni et al. (Soni et al., 2015) proposed a trust based scheme for location finding to help the driver to validate or deny the presence of the desired location. To reach this purpose, they were based on the majority voting from nearby vehicles. Hu et al. (Hu et al., 2015) introduced a trust model for relay selection to guarantee that only the most reliable nodes are selected for data transmission. The relay score that refers to the candidate trust is calculated according to the: (1) rate of successful routed messages and (2) similarity level in regard to the routed message. Dahmane et al. (Dahmane et al., 2017) also presented a weighted trust-aware relay selection scheme. They combined the vehicles' and context related information such as the distance between the transmitter and the candidate, the quality and lifetime of communication link as well as the rate of successful routed messages.

Several other trust models focus on the data trust instead of the entity trust. Raya et al. (Raya et al., 2008) were the first to investigate the message's trustworthiness in ephemeral networks. They incorporated (1) the correlative trustworthiness of the event and its reporter, (2) the security status that reflects the entity legitimacy and the (3) proximity in terms of time and location. Mazilu et al. (Mazilu et al., 2011) were also interested in the network security based on data trust computation. This model uses similarity to find out the coincidence between locally stored measurements and the others' detections. Zaidi et al. (Zaidi et al., 2014) also adopted the same methodology to validate their own measurements. They further investigated the correlation between the speed, flow and density to detect the rogue nodes that affect the quality of emergency alerts. Alike the majority of the existing trust models, all of the mentioned data-oriented trust models supposed that the trust-based decision should rely on multiple messages to confirm the reliability of the reported alert.

Regarding the hybrid trust, most of research studies combine the entity and message trust to achieve more reliable and accurate trust estimation. Usually, the entity trust represents one of the major factor to build the message's trustworthiness. Both Oluoch (Oluoch, 2015) and Yao et al. (Yao et al., 2017a) assumed that the entity trust depends on its reputation while the message trust is estimated according to the: (1) reporter's trustworthiness, (2) correlative trust of the event and its reporter and (3) both time and location. Li and Song (Li and Song, 2016) proposed an attack resistant trust scheme. They combined the: (1) functional trust and evidences from third parties to evaluate the entity trust and (2) similarity between the collected reports to validate the message's trustworthiness. Soleymani et al. (Soleymani et al., 2017) incorporated three main modules to decide whether to trust an event or not. The experience module (refers to reputation) depends on past interactions between vehicles. The plausibility module aims at verifying the correctness of the location information. The accuracy module includes fog nodes that intend to store events-related to the traffic state. Thus, whenever a vehicle receives a warning, it asks fog nodes to prove or deny the presence of the such event.

Most of the investigated trust schemes stand on reputation assessment to validate the entity's trustworthiness. Nonetheless, this methodology is not well suited in highly dynamic environments since it requires social connections that should last for a long duration. We also highlight that some of these schemes adopted predefined measurements (e.g. the correlative trust of the event and its reporter) that may affect the accuracy of the trust calculation. Moreover, most of the cited research studies adopt fuzzy logic and probability theory to cope with the information uncertainties in VANETs. Some of these models use fuzzy logic theory to compute trust based on basic parameters such as time, position, etc. (Mármol and Pérez, 2012) (Soleymani et al., 2017). To the best of our knowledge, none of the existing research addressed the trustworthiness of the energy-related information for EVs. In fact, electric vehicular networks have the same characteristics as VANETs. However, they have additional restrictions, mainly the energy-related constraints. Accordingly, in this paper we introduce a new fuzzy-based trust model that relies on the similarity assessment between messages in terms of energy consumption. This model aims at filtering the inappropriate reports in order to ensure that only plausible measurements are considered to provide high quality of services.

3 PROBLEM DEFINITION

Nowadays, the emergence of cellular technologies (e.g. 4G, 5G) and open WiFi access points enable vehicles to directly communicate with the network (V2N communication) particularly, with centralized servers (Wang et al., 2014). In this paper, we assume that the main roles of the server are to: (1) help the driver to follow the optimal path (in terms of energy consumption, time and distance) and (2) decide whether its battery state allows him to reach its destination, depending on the traffic state, or not. To reach this purpose, the server analyses and processes messages from multiple dispersed vehicles in order to mitigate the inherent security risks that may affect the quality of the provided services.

Often, the network includes (1) credible entities that behave properly and (2) malicious vehicles that misbehave due to selfish reasons, sensors' failure, etc. These bad entities broadcast erroneous information about their position, speed, energy consumption, etc. Our model addresses the following types of security threats as depicted in Figure 2 (Sumra et al., 2015):

- Sybil attack: sends multiple messages under different identities and from different locations to lie about the real traffic state.
- Fake information attack: injects erroneous information about its speed, energy, etc. For example, a vehicle says that it runs with a low speed and it consumes a big amount of energy to discourage the other vehicles to follow the same lane.
- Timing attack: creates a delay to prevent the server from receiving real-time information.
- Selective forwarding attack: forwards messages with low interest. For example a vehicle may only transmit messages whenever it consumes energy (i.e. denies that it recovers energy in downhill roads) in order to say that the followed lane is greedy in terms of energy consumption.
- On-off attack: behaves alternatively to maintain the same level of trust. For example, a vehicle transmits an accurate energy consumption value at time *t-1* and thereafter, it lies about the consumed energy between the two instants *t-1* and *t*.
- Bush telegraph attack: applies a slight modification, that cannot be perceived, to the right measurement. For example, whenever a vehicle sends its energy consumption between two instants, it executes a slight modification to deceive the server in identifying the optimal path.
- Collusion attack: a set of vehicles collude to reach the same purposes. For example, they lie about the energy consumption on a specific lane to convince the server that this lane is greedy in terms of energy consumption.

We highlight that there is a crucial need to propose an effective and reliable trust management scheme that mainly deals with energy-related issues for EVs.

The main role of this scheme is to maintain the quality of the provided services (e.g. ensure that only trusted messages contribute during the identification of the optimal path).

4 SIMILARITY-BASED TRUST ESTIMATION MODEL FOR ELECTRIC VEHICLES

In electric vehicular networks, each vehicle periodically transmits its ID, position, speed, etc. (the structure of the message is depicted in Figure 1) to enable the server to estimate the shortest path in terms of energy consumption, distance and travel time. Subsequently, we should underline that the server does not have prior knowledge about the required energy for the driver's path due to the variation of the: (1) traffic condition, (2) and the state of the environment (e.g. accident, work-zone, heavy rain or snow).

Vehicle's ID	Lane ID	Position (x, y)	Transmission Time	Speed	Instant Energy

Figure 1: Structure of the transmitted message.

In this paper, we present a new trust model to allow the server to filter the received messages as shown in Figure 2. Based on this model, the server will only consider plausible and trusted messages. Firstly, it starts by grouping vehicles that belong to the same lane. Accordingly, it is required to evaluate the accuracy of the reported lane as well as the vehicle's position. Thereafter, the server verifies the message validity to identify the outdated ones. Afterwards, it evaluates the trustworthiness of the reported speed. As the focus of this paper is on the accuracy of the reported consumed energy for EVs, then we will stand on existing works for position, time and speed verification as referred in (Yang, 2013) (Soleymani et al., 2017) (Yao et al., 2017b).

Subsequently, the server assesses the reliability of the reported energy consumption at each instant based on the: (1) vehicle's behavior (i.e. accelerates or decelerates) and (2) correlation between the speed variation and the sign of energy. The aim behind the instant energy verification is to filter messages coming from malicious vehicles that broadcast false energy information. At the last step, the server evaluates the similarity between the overall reported energy, by each vehicle, on each lane according to: (1) the vehicle's position regarding the lane, and (3) the correlation between the average speed and the consumed energy. In this stage, the server can detect the bush telegraph, on-off and selective forwarding attacks.

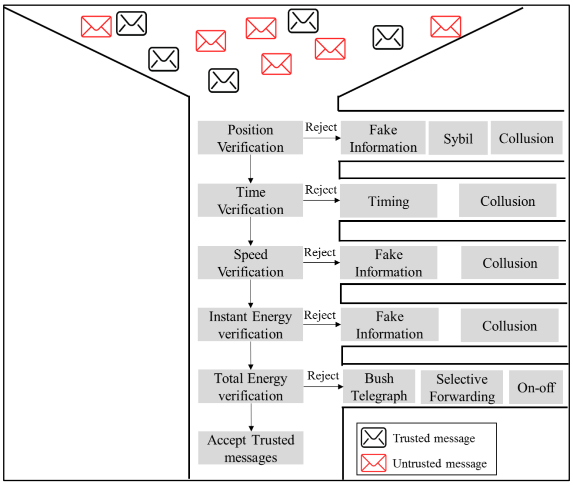

Figure 2: Overview of the proposed model.

This model can effectively deal with several kinds of threats (as depicted in Figure 2). The similarity assessment between messages in terms of all of the aforementioned parameters (position, time, speed and energy) allows the server to identify and reject messages coming from malicious EVs. We underline that this model is time-effective since it can speed up the selection of the most trusted messages based on a sequential filtering. That is to say that whenever the server detects weird and incredible information, it directly rejects them without the need to pass through the other steps. We also underline that the fuzzy logic theory can effectively evaluate the message's trustworthiness in terms of energy consumption. The reason behind the use of such theory is because of its ability to: (1) deal with fuzzy, uncertain and imprecise measurements and (2) transform uncertain and imprecise information into precise and accurate results. In the next section, we present and detail the role of fuzzy logic to differentiate between trustworthy and untrustworthy messages.

5 FUZZY-BASED TRUST ASSESSMENT APPROACH

In this section, we detail the proposed fuzzy-based model for energy trust assessment. Indeed, fuzzy logic is able to transform the information-based perception into information-based accurate measurements (Klir and Yuan, 1995) (Zadeh, 2004). This theory consists of three main phases:

- Fuzzification: converts the real domain into fuzzy domain. At this stage, it is required to specify the system's inputs/ outputs, the size of the universe of discourse, the fuzzy classes and membership functions (Klir and Yuan, 1995).

- Inference: there are three main inference methods: min-max method, max-prod method and sum-prod method (Klir and Yuan, 1995). In this paper, we use the min-max method since it is the most commonly used one due to its simple structure. The inference process aims to represent the correlation between the inputs and outputs using the fuzzy rules.
- Defuzzification: transforms the fuzzy domain into accurate and precise domain. Several defuzzification methods exist in the literature: bisector method, mean of maxima method and centroid method (Saade and Diab, 2004). In this paper, we use the centroid method since it provides more effective results than the other models (Saade and Diab, 2004). The centroid is computed as follows:

$$Centroid = \frac{\int x_i\, \mu(x_i)}{\int \mu(x_i)}$$

x_i and $\mu(x_i)$ denote the fuzzy value and aggregated membership function, respectively.

5.1 Assumptions

Our fuzzy-based trust model considers a set of assumptions as follows:

(a) Each vehicle periodically sends its energy consumption.

(b) The vehicle's ID remains static until the vehicle moves from one lane to another.

(c) The number of malicious entities that collude to affect the instant/ total energy consumption should not exceed the number of legitimate entities.

(d) The number of vehicles that belong to the same lane is greater than two.

(e) The energy trust is estimated for the same type of electric vehicles.

(f) Only trusted messages in terms of position, transmission time and speed are handled during the energy verification.

(g) The speed is the most influential factor that has a great impact on the energy consumption for EVs (Badin et al., 2013). The more the *EV* accelerates or decelerates, the higher the energy consumed or recovered, respectively.

5.2 Description of the Proposed Model

In this subsection, we detail the presented model for the: (1) Instant Energy Verification (IEVer) and, (2) Total Energy Verification (TEVer) in order to ensure that only trusted energy information is considered by the server. Both IEVer and TEVer processes are instantly triggered (i.e. at each time *t*) to cope with false energy information. IEVer cannot address, alone, to the whole energy verification problem since the vehicle's behavior may evolve over time (e.g. $send/no-send/send$ behavior). Accordingly, the TEVer is required to verify that the vehicle, always, behaves properly throughout the lane.

To accomplish the IEVer and TEVer, we use the fuzzy logic theory so as to evaluate the similarity level between each input and the corresponding median value. We state that the use of the median strategy can better reflect the energy trust than the mean strategy. Actually, this latter may distinctly deviate if malicious vehicles provide wrong information that extensively differs from real information. In fact, the median is a commonly used strategy in statistics and probability theory (Cadenas et al., 2012). It depends on the sample size as well as the reported values (e.g. energy consumption). Accordingly, the establishment of fuzzy classes, for each input, is strongly related to the estimation of the median value. We should also underline that fuzzy classes are dynamically established to deal with the specifications of each road type (highway, urban zone, etc.) as well as the traffic density.

IEVer: Instant Energy Verification. Initially, the server checks the coincidence between the reported energy consumption and the speed variation between two instants *t-1* and *t*. Therefore, if an electric vehicle EV_i accelerates or decelerates and the reported energy is negative or positive respectively then, EV_i is classified as malicious. However, only based on the coincidence between the speed variation and the sign of energy, we cannot ensure that the reported energy is absolutely accurate since a malicious *EV* may lie about the amount of the consumed/ recovered energy. For example, a vehicle may accelerate a little bit but, it indicates that it consumes a high amount of energy that mismatch with its acceleration rate. Therefore, we use the fuzzy logic to deal with such situation and decide whether the reported energy is appropriate or not. The process for the IEVer is given in Algorithm 1.

In this study, we consider the coincidence between: (1) the Acceleration (*A*) and the Consumed Energy (*CE*) where *A* and *CE* are positive, and (2)

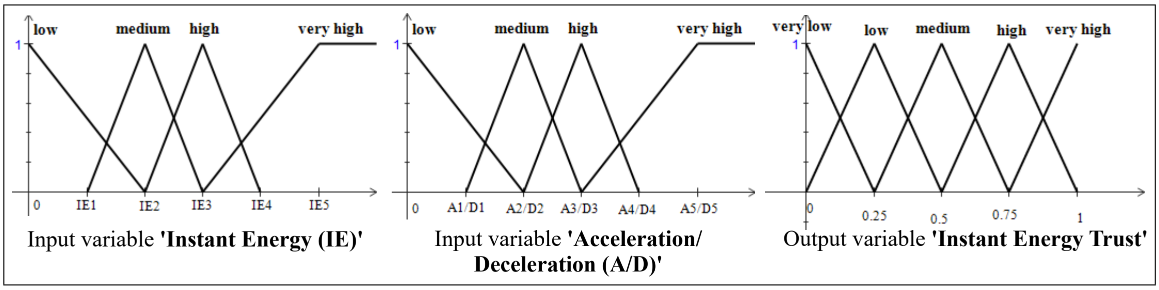

Figure 3: Fuzzy classes and membership functions for IEVer.

Algorithm 1: Detect untrustworthy messages in regard to Instant Energy.

```
for each received message $m$ at time $t$ do     % $m$ is trusted in regard to the speed
1. Verify the coincidence between the speed variation and the sign of energy
Extract the speed ($S_{t-1}$) and ($S_t$) at time $t$-$1$ and $t$
Extract the instant energy consumption ($IE$) between $t$-$1$ and $t$
if (($S_t$)-($S_{t-1}$)≥0) then                  % Vehicle accelerates
  if ($IE$ ≥0) then $m$ is probably trustworthy  % Vehicle consumes energy
    else $m$ is untrustworthy
  end if
    else                                         % Vehicle decelerates
      if ($IE$ ≥0) then $m$ is untrustworthy
        else $m$ is probably trustworthy         % Vehicle recovers energy
      end if
end if
2. Apply the fuzzy logic to identify the untrustworthy messages
Determine the median Consumed/ Recovered Energy and the corresponding Acceleration/ Deceleration rate
Build the Fuzzy Classes (FCs) and membership functions (refer to Figure 3)
Build the rule base (refer to Table 1)
Apply the defuzzification method
if (Trust($IE$)≥Threshold) then $m$ is trustworthy
  else $m$ is untrustworthy
end if
end for
```

the Deceleration (D) and the Recovered Energy (RE) where D and RE are negative. Indeed, in electric vehicular networks, EVs are designed to recover energy whenever the vehicle decelerates or goes downhill. Therefore, in our model, we create two Fuzzy Inference Systems (FIS). The first FIS is dedicated to check the reliability of CE while the second one is interested in the trust evaluation of RE. However, we suppose that the Instant Energy (IE) for CE and RE can be both modeled similarly (IE{CE} = $|IE\{RE\}|$) as shown in Figure 3. As well, both A and D can be represented in the same figure (A = $|D|$). Accordingly, our FIS considers the acceleration/ deceleration and the instant consumed/ recovered energy as the system's inputs and the instant energy trust as the output.

We suppose that Fuzzy Classes (FCs) are dynamically established according to the traffic state. In fact, FCs for IE depend on the median energy value as described below:

$$\begin{cases} FC1: [0,\ 0,\ IE_2] & \\ FC2: [IE_1,\ IE_2,\ IE_3] & IE_1 = IE_2/2 \\ & IE_3 = IE_1 + IE_2 \\ FC3: [IE_2,\ IE_3,\ IE_4] & IE_4 = 2 * IE_2 \\ FC4: [IE_3,\ IE_5,\ +\infty,\ +\infty[& IE_5 = IE_4 + IE_1 \end{cases}$$

IE_2 refers to the median consumed/ recovered energy at time t. Regarding the fuzzy classes for A/D, they are determined in correspondence with the identified classes for IE. Particularly, for each $IE_i\{CE/RE\}$ value, our solution identify the convenient A_i/D_i rate as depicted in Figure 3.

Based on the used inputs, we propose the rule table (Table 1) that includes sixteen rules. This value depends on the number of the inputs (two inputs) and the corresponding fuzzy sets (four fuzzy sets for each input: low, medium, high, very high). Table 1 represents the correlation between the inputs and the output. It illustrates that A/D should be proportional to $IE\{CE/RE\}$. For example, if the consumed/ recovered energy is below the computed median value IE_2, then the vehicle's acceleration/ deceleration should not exceed A_2/D_2.

Algorithm 1 shows that if the computed trust value is below a defined threshold, then the message will be discarded. Therefore, only trustworthy messages in regard to instant energy will be handled in the next step. We highlight that, although the IEVer allows the detection of wrong energy information, EVs may launch other kinds of threats that cannot be supported by the IEVer alone. Next, we show the need of the TEVer to detect the bush telegraph, on-off and selective forwarding attacks in order to enhance the quality of the provided services.

TEVer: Total Energy Verification. TEVer aims at ensuring that EVs have not lied at all. Therefore, only the most appropriate total energy consumption is considered by the server. Algorithm 2 is adopted to measure the trust in the total energy consumption by each

Table 1: Fuzzy rules for IEVer.

Rule	Input A/D	Input IE	Output Trust(IE)	Rule	Input A/D	Input IE	Output Trust(IE)
1	low	low	very high	9	high	low	very Low
2	low	medium	high	10	high	medium	medium
3	low	high	low	11	high	high	very high
4	low	very high	very low	12	high	very high	medium
5	medium	low	high	13	very high	low	very low
6	medium	medium	very high	14	very high	medium	low
7	medium	high	medium	15	very high	high	medium
8	medium	very high	very low	16	very high	very high	high

Algorithm 2: Detect untrustworthy messages in regard to Total Energy.

```
for each received message $m$ at time $t$ do                    % $m$ is trusted in regard to $IE$
Extract the speed ($S_t$) at time $t$
Extract the energy consumption ($E_t$) between $t$-$1$ and $t$
if ($laneID_{t-1}$==$laneID_t$) then                % Vehicle still belongs to the same lane
  $AS_t$=($nAS_{t-1}$+$S_t$)/($n+1$)            % Update the average speed
   $TE_t$=$TE_{t-1}$+$E_t$                    % Update the total energy consumption
  else                                      % Vehicle moves to a new lane
    $AS_t$=$S_t$                            % Initialize the average speed
     $TE_t$=$E_t$                           % Initialize the total energy consumption
end if
Extract the coordinates of the involved lane ($X_{min}$, $X_{max}$)
% $X_{min}$ refers to the start abscissa and $X_{max}$ refers to the end abscissa
Determine the median of the Total Energy Consumption ($TE\_Med$) and the corresponding Average speed ($AS\_Med$)
Build the Fuzzy Classes (FCs) and membership functions (refer to Figure 4)
Build the rule base (refer to Table 2)
Apply the defuzzification method
if (Trust($TE$)≥Threshold) then $m$ is trustworthy
  else $m$ is untrustworthy
end if
end for
```

EV throughout a specific lane.

In this study, the proposed FIS for TEVer takes three inputs into consideration: (1) the vehicle's position in regard to the lane (Pos_{lane}), the average speed (AS), and the total energy consumption (TE). The output of this FIS is the total energy trust (Trust(TE)). Regarding the Pos_{lane}, the range is between X_{min} and X_{max} that, respectively, refer to the starting and ending abscissa. FCs for Pos_{lane} are described as follows:

$$\begin{cases} FC1 : [X_{min},\, X_{min},\, X_2] & X_2 = (3/4)X_3 \\ FC2 : [X_1,\, X_2,\, X_4] & X_1 = (1/4)X_3 \\ & X_4 = X_1 + X_3 \\ FC3 : [X_2,\, X_4,\, X_5] & X_5 = X_2 + X_3 \\ FC4 : [X_4,\, X_4,\, X_{max}] & \end{cases}$$

X_3= (X_{max}-X_{min})/2 is the basis of the FCs establishment for the parameter Pos_{lane}. It refers to the midpoint of the lane and it depends on its length. In regard to TE, the range is between 0 and $+\infty$. FCs are defined as follows:

$$\begin{cases} FC1 : [0,\, 0,\, TE_1] & TE_1 = TE_2/2 \\ FC2 : [0,\, TE_1,\, TE_2] & \\ FC3 : [TE_1,\, TE_2,\, TE_3] & TE_3 = TE_1 + TE_2 \\ FC4 : [TE_2,\, TE_3,\, TE_4] & TE_4 = 2 * TE_2 \\ FC5 : [TE_3,\, TE_4,\, TE_5] & TE_5 = TE_1 + TE_4 \end{cases}$$

TE_2 is the median value for the total energy consumption. It represents the basis of the specification of FCs. If TE exceeds the value TE_5, then TE will be directly rejected. Regarding the AS range, it varies from the minimum to the maximum reported speed. For the sake of simplicity, we suppose that the maximum range tends to infinity ($+\infty$). We should remind that only trusted messages in terms of speed information are considered in the TEVer process. Fuzzy classes for AS are dependent upon the median value for TE_2. That is to say that, after the estimation of the median value for TE, we can identify its equivalent in terms of AS. Therefore, the proposed FCs for AS can be described as below:

$$\begin{cases} FC1 : [AS_{min},\, AS_{min},\, AS_2] & \\ FC2 : [AS_1,\, AS_2,\, AS_3] & AS_1 = AS_{min} + \\ & [(AS_2 - AS_{min})/2] \\ & AS_3 = AS_1 + AS_2 \\ FC3 : [AS_2,\, AS_4,\, +\infty,\, +\infty[& AS_4 = 2 * AS_2 \end{cases}$$

AS_{min} refers to the minimum followed speed at the involved lane while AS_2 is the equivalent speed to the median TE (i.e. TE_2). For example, we suppose that a set of vehicles are dispersed throughout a specific lane. Therefore, if a vehicle runs with AS_2 then, it usually consumes around TE_2 whenever it reaches a particular position in the lane (near to X_3). Table 2 illustrates the dependencies between the suggested parameters (Pos_{lane}, AS, TE and Trust(TE)). This table shows that TE should be proportional to AS and Pos_{lane}. Actually, our study considers the vehicle's position into consideration since it can provide additional information about the reliability of the energy consumption. For example, two vehicles EV_1 and EV_2

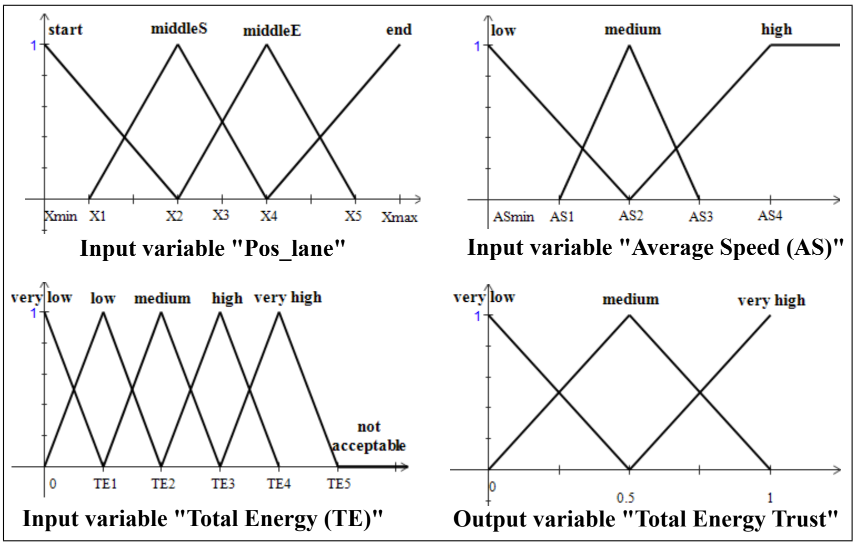

Figure 4: Fuzzy classes and membership functions for TEVer.

follow the same lane. EV_1 is still in the beginning of the lane while EV_2, almost, reaches the end of the same lane. Therefore, EV_1 and EV_2 should not consume the same amount of energy although they run with the same average speed.

In brief, the proposed fuzzy-based trust model consists of two main phases (IEVer and TEVer) to enable the server to filter the inappropriate energy-related information. In each phase, we use fuzzy logic to detect wrong energy information that mismatches with the vehicle's behavior in terms of acceleration/ deceleration rate and average speed. In the next section, we evaluate the performance of the proposed model versus several kinds of threats.

6 PERFORMANCE EVALUATION

In this section, the performance of the proposed fuzzy-based trust model is evaluated in regard to the consistency of the energy consumption. Accordingly, we are interested in the energy-related threats as shown in Figure 2. Therefore, we mainly focus on the fake information, bush telegraph, selective forwarding, on-off and collusion attacks. We use *MATLAB* to create a fuzzy-based inference engine and *SUMO* to generate traffic data (Krajzewicz et al., 2006). *SUMO* provides a set of files that include information related to each vehicle in every simulation time step such as the vehicle's ID, the consumed energy between two time steps, the actual battery capacity, the speed, etc. In our simulation, we suppose that the length of the lane segment is equal to *2000m*. We also conduct simulations for *100s* where each step takes around *1s*. Regarding the number of vehicles, it varies from *n=10* to *n=100*. Finally, we set the threshold to the neutral value *0.5* (i.e. if the trust value is below *0.5* then the message is suspicious otherwise, it is trustworthy).

Figure 5 illustrates the correlation between the inputs (A and IE) and output (Trust(IE)). We suppose that A and IE vary from $0m/s^{-2}$ to $1m/s^{-2}$ and from $0W$ to $10W$, respectively. We also suppose that the median value for IE is equal to $4W$ and the corresponding acceleration is equal to $0.3m/s^{-2}$. Accordingly, Figure 5 shows that trust increases whenever A and IE are proportional.

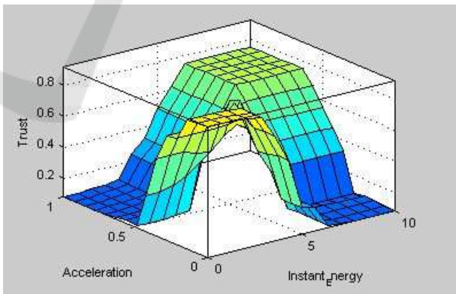

Figure 5: Correlation between inputs and output for IEVer.

We notice that, if A and IE vary from $0m/s^{-2}$ to $0.5m/s^{-2}$ and from $0W$ to $6W$ respectively, then trust is increasingly high. However, if A is between $0.5m/s^{-2}$ and $1m/s^{-2}$, and IE is between $0W$ and $4W$, then trust is between 0.08 and 0.25. Therefore, the more the EV accelerates, the higher the IE should be and, subsequently, the more the Trust(IE) increases.

Figure 6 depicts the correlation between the inputs (Pos_{lane} AS and TE) and output (Trust(TE)). This

Table 2: Fuzzy rules for TEVer.

Rule	Input	Input AS	Input TE	Output	Rule	Input	Input AS	Input TE	Output
	Pos_{lane}			Trust(TE)		Pos_{lane}			Trust(TE)
1	start	low	very low	high	31	middleE	low	very low	low
2	start	low	low	medium	32	middleE	low	low	low
3	start	low	medium	low	33	middleE	low	medium	high
4	start	low	high	low	34	middleE	low	high	medium
5	start	low	very high	low	35	middleE	low	very high	low
6	start	medium	very low	medium	36	middleE	medium	very low	low
7	start	medium	low	high	37	middleE	medium	low	low
8	start	medium	medium	low	38	middleE	medium	medium	medium
9	start	medium	high	low	39	middleE	medium	high	high
10	start	medium	very high	low	40	middleE	medium	very high	low
11	start	high	very low	low	41	middleE	high	very low	low
12	start	high	low	high	42	middleE	high	low	low
13	start	high	medium	medium	43	middleE	high	medium	medium
14	start	high	high	low	44	middleE	high	high	high
15	start	high	very high	low	45	middleE	high	very high	low
16	middleS	low	very low	medium	46	end	low	very low	low
17	middleS	low	low	high	47	end	low	low	low
18	middleS	low	medium	low	48	end	low	medium	medium
19	middleS	low	high	low	49	end	low	high	high
20	middleS	low	very high	low	50	end	low	very high	low
21	middleS	medium	very low	low	51	end	medium	very low	low
22	middleS	medium	low	high	52	end	medium	low	low
23	middleS	medium	medium	medium	53	end	medium	medium	low
24	middleS	medium	high	low	54	end	medium	high	high
25	middleS	medium	very high	low	55	end	medium	very high	medium
26	middleS	high	very low	low	56	end	high	very low	low
27	middleS	high	low	medium	57	end	high	low	low
28	middleS	high	medium	high	58	end	high	medium	low
29	middleS	high	high	low	59	end	high	high	medium
30	middleS	high	very high	low	60	end	high	very high	high

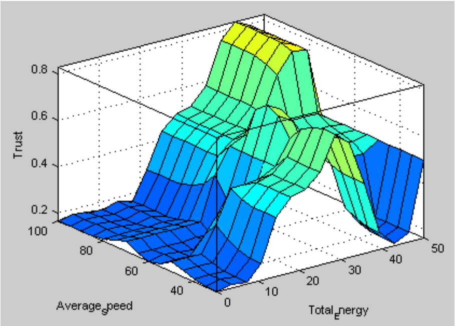

Figure 6: Correlation between inputs and output for TEVer.

figure shows that AS and TE vary from $30km/h$ to $100km/h$ and from $0W$ to $50W$, respectively. We suppose that the median value for TE is equal to $20W$ and the corresponding AS is equal to $60km/h$. We further suppose that the vehicle almost reaches the end of the lane ($Poslane$=1900m).

Accordingly, whenever the vehicle reaches the end of the lane, then trust seems to be high (around 0.82) only if AS and TE are proportional. For example, we notice that if AS is between $30km/h$ ($ASmin$) and $100km/h$ ($ASmax$) and TE between $0W$ and $30W$ then trust does not exceed 0.4 since the EV is in the end of the lane (Pos_{lane}=1900m). However, in regard to the same position, if AS and TE vary from $75km/h$ to $100km/h$ and from $40W$ to $50W$ respectively, then trust can reach 0.83. Nevertheless, if TE exceeds $50W$ then, trust decreases regardless the AS.

We perform a series of experiments for different percentages of false messages (*P=10%, 25%, 40%*) and with/without collusion attack to evaluate the precision of the proposed IEVer solution as illustrated in Figure 7. We should also highlight that false readings are randomly generated. Simulation results show that IEVer performs well to detect the misbehaving entities that provide wrong energy information that mismatches with their acceleration or deceleration rate. Viewed from Figure 7, it is obvious that the IEVer resists to the false data injection attack with/without collusion and achieves a high precision regardless the number of vehicles that belong to the same lane.

Moreover, we notice that the detection of the collusion attack is achieved with higher precision compared with the absence of such attack since all of bad entities collude to provide similar wrong energy information (i.e. very low/ very high energy consumption). That is to say that some vehicles, that consume a small/big amount of energy, collude to convince the server that they consume a big/small amount of energy, respectively. In such situation, these entities can be detected with a high precision that usually reaches *98%*. In the second instance (i.e. without collusion), each vehicle independently lies about its energy. In this case, the detection of bad entities is reduced a little bit due to the dynamicity of fuzzy classes. We also notice that the detection of false data injection attack is moderately accomplished with around *87%* (if *n=10* and *P=40%*) and *90%* (if *n=100* and *P=40%*) since the rate of wrong messages has lower impact on the selection of the median energy in high traffic density compared with in low traffic density.

However, the IEVer cannot resist to the bad entities that: (1) consume high amount of energy but they pretend that they consume much more, (2) attribute a slight modification of their real energy consumption (i.e. Bush telegraph) in each time step or, (3) selectively forward their energy consumption (i.e. selective forwarding or on-off). To overcome these limitations, we propose to evaluate the accuracy of the overall energy consumption (TEVer).

Figure 8 shows that TEVer is effective to overcome these limitations. First, we should underline that the more the vehicle is approaching to the end of the lane, the better the detection of malicious nodes. In Figure 8 we conduct different experiments to prove that TEVer deals with the On-off attack in different scenarios: (1) $send/send/no-send$, (2) $send/no-send/send$ and (3) $no-send/no-send/send$. According to Figure 8, it is obvious that TEVer allows the detection of the on-off attack with high precision, especially for the case $no-send/no-send/send$ (higher than *92%*). In this case, the detection of such attack is very effective since the total consumed energy is very low compared with the expected one. Hence, the more the vehicle behaves improperly, the higher the precision. Moreover, we notice that whenever the traffic density increases (*n=100* and *P=40%*), the precision increases simultaneously compared with in low traffic density (*n=10* and *P=40%*). This can be explained by the fact that, for the same percentage of malicious vehicles, the identification of the median total energy consumption is more accurate in high traffic density than low traffic density. Similarly, we believe that TEVer is effective to deal with the selective forwarding attack since it almost behaves like the on-off attack.

Regarding the bush telegraph attack, we perform multiple experiments with different α values as depicted in Figure 9. α refers to the variation rate of the real consumed energy that can increase (+α) or decrease (-α). Indeed, TEVer is more effective with the bush telegraph attack that provides high energy information (+α) than the bush telegraph attack that reduces the real energy consumption (-α) especially when α=20% and α=30%. Figure 9 shows also that the more the total energy deviates (i.e. α increases), the higher the precision. Moreover, we notice that the detection of this attack is improved whenever the traffic density increases since the number of false messages has lower effect on the establishment of fuzzy classes in the second instance (i.e *n=100*) compared with the first one (i.e. *n=10*). Therefore, in regard to the same percentage of false messages (e.g. *P=25%*), we notice that for *n=10*, the precision is around *50%* and for *n=100*, the precision reaches *70%*.

In summary, we can deduce that the proposed model for IEVer and TEVer is resilient to multiple threats in different traffic densities. This model provides a high protection against the malicious entities that misbehave due to selfish, malicious and unintentional reasons.

7 CONCLUSION AND FUTURE WORK

In this paper, a new fuzzy-based trust model was proposed to evaluate the accuracy of the energy information reported by electric vehicles. The proposed solution consists of two main dimensions: the instant energy verification and total energy verification. The aims of this model are mainly to (1) filter the wrong energy information that mismatches with the vehicle's behavior (e.g. acceleration and deceleration) and (2) ensure that only credible and plausible information is considered to enhance the quality of the provided services in electric vehicular networks. Results and analysis prove the effectiveness of the proposed solution to detect several kinds of threats, that broadcast wrong energy information, in different traffic densities. As future work, we intend to propose a self-adaptive trust model for electric vehicular networks. The purpose of this model is to adopt the convenient methodologies for trust assessment, according to the context and the

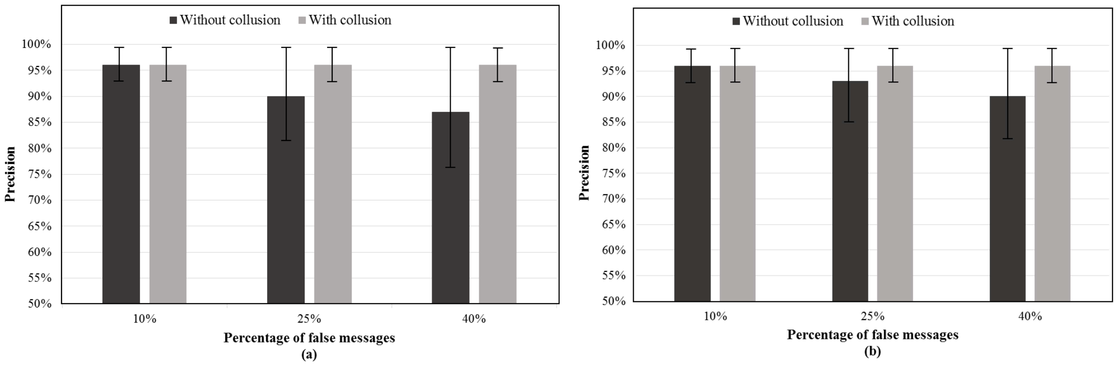

Figure 7: Performance of IEVer versus the false data injection attack (with/without collusion attack). Precision for (a) n=10 and (b) n=100.

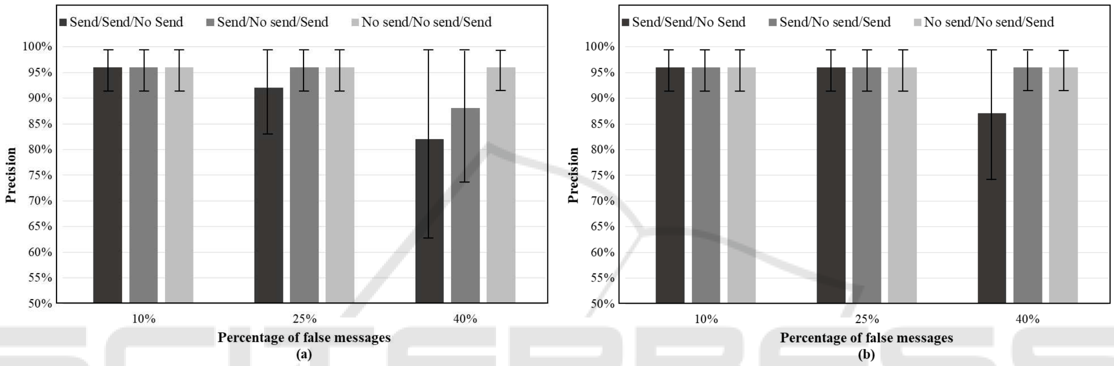

Figure 8: Performance of TEVer versus the On-off attack. Precision for (a) n=10 and (b) n=100.

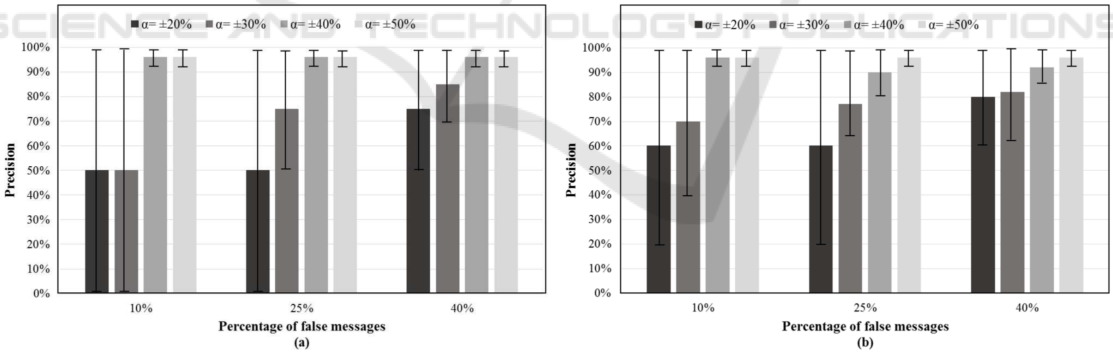

Figure 9: Performance of TEVer versus the Bush Telegraph attack. Precision for (a) n=10 and (b) n=100.

characteristics of the provided applications.

ACKNOWLEDGEMENTS

This work was supported by the PHC Utique program of the French Ministry of Foreign Affairs and Ministry of higher education and research and the Tunisian Ministry of higher education and scientific research in the CMCU project number 16G1404.

REFERENCES

Al-Kahtani, M. S. (2012). Survey on security attacks in vehicular ad hoc networks (vanets). In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, pages 1–9. IEEE.

Alam, K. M., Saini, M., and El Saddik, A. (2015). Toward social internet of vehicles: Concept, architecture, and applications. *IEEE Access*, 3:343–357.

Badin, F., Le Berr, F., Briki, H., Dabadie, J., Petit, M., Magand, S., and Condemine, E. (2013). Evaluation of evs energy consumption influencing factors, driving conditions, auxiliaries use, driver's aggressiveness. In *Electric Vehicle Symposium and Exhibition (EVS27), 2013 World*, pages 1–12. IEEE.

Bayram, I. S. and Papapanagiotou, I. (2014). A survey on communication technologies and requirements for internet of electric vehicles. *EURASIP Journal on Wireless Communications and Networking*, 2014(1):223.

Cadenas, J., Megson, G. M., Sherratt, R., and Huerta, P. (2012). Fast median calculation method. *Electronics letters*, 48(10):558–560.

Dahmane, S., Kerrache, C. A., Lagraa, N., and Lorenz, P. (2017). Weistars: A weighted trust-aware relay selection scheme for vanet. In *Communications (ICC), 2017 IEEE International Conference on*, pages 1–6. IEEE.

Falk, R. and Fries, S. (2012). Electric vehicle charging infrastructure security considerations and approaches. *Proc. of INTERNET*, pages 58–64.

Hu, H., Lu, R., and Zhang, Z. (2015). Vtrust: a robust trust framework for relay selection in hybrid vehicular communications. In *Global Communications Conference (GLOBECOM), 2015 IEEE*, pages 1–6. IEEE.

Klir, G. and Yuan, B. (1995). *Fuzzy sets and fuzzy logic*, volume 4. Prentice hall New Jersey.

Krajzewicz, D., Bonert, M., and Wagner, P. (2006). The open source traffic simulation package sumo. *RoboCup 2006*.

Li, W. and Song, H. (2016). Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 17(4):960–969.

Mármol, F. G. and Pérez, G. M. (2012). Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35(3):934–941.

Mazilu, S., Teler, M., and Dobre, C. (2011). Securing vehicular networks based on data-trust computation. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2011 International Conference on*, pages 51–58. IEEE.

Oluoch, J. O. (2015). *A unified framework for trust management in Vehicular Ad Hoc Networks (VANET)*. PhD thesis, Oakland University.

Raya, M., Papadimitratos, P., Gligor, V. D., and Hubaux, J.-P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1238–1246. IEEE.

Saade, J. J. and Diab, H. B. (2004). Defuzzification methods and new techniques for fuzzy controllers.

Soleymani, S. A., Abdullah, A. H., Hassan, W. H., Anisi, M. H., Goudarzi, S., Baee, M. A. R., and Mandala, S. (2015). Trust management in vehicular ad hoc network: a systematic review. *EURASIP Journal on Wireless Communications and Networking*, 2015(1):146.

Soleymani, S. A., Abdullah, A. H., Zareei, M., Anisi, M. H., Vargas-Rosales, C., Khan, M. K., and Goudarzi, S. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access*, 5:15619–15629.

Soni, S., Sharma, K., and Chaurasia, B. K. (2015). Trust based scheme for location finding in vanets. In *Advances in Optical Science and Engineering*, pages 425–432. Springer.

Sumra, I. A., Hasbullah, H. B., and AbManan, J.-l. B. (2015). Attacks on security goals (confidentiality, integrity, availability) in vanet: a survey. In *Vehicular Ad-Hoc Networks for Smart Cities*, pages 51–61. Springer.

Sun, S.-h., Hu, J.-l., Peng, Y., Pan, X.-m., Zhao, L., and Fang, J.-y. (2016). Support for vehicle-to-everything services based on lte. *IEEE Wireless Communications*, 23(3):4–8.

Wang, C.-X., Haider, F., Gao, X., You, X.-H., Yang, Y., Yuan, D., Aggoune, H., Haas, H., Fletcher, S., and Hepsaydir, E. (2014). Cellular architecture and key technologies for 5g wireless communication networks. *IEEE Communications Magazine*, 52(2):122–130.

Wei, Z., Yu, F. R., and Boukerche, A. (2014). Trust based security enhancements for vehicular ad hocnetworks. In *Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications*, pages 103–109. ACM.

Yang, N. (2013). A similarity based trust and reputation management framework for vanets. *International Journal of Future Generation Communication and Networking*, 6(2):25–34.

Yao, X., Zhang, X., Ning, H., and Li, P. (2017a). Using trust model to ensure reliable data acquisition in vanets. *Ad Hoc Networks*, 55:107–118.

Yao, Y., Xiao, B., Wu, G., Liu, X., Yu, Z., Zhang, K., and Zhou, X. (2017b). Voiceprint: A novel sybil attack detection method based on rssi for vanets. In *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on*, pages 591–602. IEEE.

Zadeh, L. A. (2004). A note on web intelligence, world knowledge and fuzzy logic. *Data & Knowledge Engineering*, 50(3):291–304.

Zaidi, K., Milojevic, M., Rakocevic, V., and Rajarajan, M. (2014). Data-centric rogue node detection in vanets. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*, pages 398–405. IEEE.

Zhang, J. (2011). A survey on trust management for vanets. In *Advanced information networking and applications (AINA), 2011 IEEE international conference on*, pages 105–112. IEEE.