Ad Hoc & Sensor Wireless Networks, Vol. 0, pp. 1–23
Reprints available directly from the publisher
Photocopying permitted by license only

Trust On the Security of Wireless Vehicular Ad-hoc Networking

DANDA B. RAWAT[1], GONGJUN YAN[2], BHED B. BISTA[3] AND MICHELE C. WEIGLE[4]

[1]*Department of Electrical Engineering, Georgia Southern University, USA*
E-mail: db.rawat@ieee.org
[2]*Department of Computer Science, University of Southern Indiana, USA*
[3]*Faculty of Software & Information Science, Iwate Prefectural University, Japan*
[4]*Department of Computer Science, Old Dominion University, USA*

Received: June 16, 2013. Accepted: February 13, 2014.

Vehicular Ad-hoc Network (VANET) security is one of the central issues in vehicular communications since each vehicle has to rely on messages sent out by the peers where the received message could be malicious. In order to protect VANETs from malicious actions, each vehicle must be able to evaluate, decide and react locally on the information received from other vehicles. In this paper, we analyze probabilistic and deterministic approaches (individually and combined) to estimate trust for VANET security. The probabilistic approach determines the trust level of the peer vehicles based on received information. The trust level is used to determine legitimacy of the message, which is used to decide whether the message would be considered for further transmission over the VANET or dropped. The deterministic approach measures the trust level of the received message by using distances calculated using received signal strength (RSS) and the vehicle's geolocation (position coordinate). Combination of probabilistic and deterministic approach gives better results compared to individual approaches. The proposed algorithms are illustrated with numerical results obtained from simulations.

Keywords: Vehicular Ad hoc network, trust for VANET security

1 INTRODUCTION

Vehicular Ad hoc NETwork (VANET) is regarded as a backbone of Intelligent Transportation System (ITS) where security and privacy issues are

still in a very early stage of development. Especially the issue of trustworthiness of the message received from other vehicles is an open question: How can one vehicle trust a message it receives from another one? By forwarding upcoming traffic information, wireless communications in VANET is expected to help reduce road accidents and fuel consumption. Note that road traffic crashes are one of the largest problems being faced not only in the US but also all over the world. A report published by National Highway Traffic Safety Administration (NHTSA) in 2012 estimates that one person dies in a vehicle crash every 15 minutes in the US [1]). Similarly, in 2006 in the US, 3.6 billion work-hours and 5.7 billion gallons of fuel wasted just because of traffic jams and congestion [14,19,25]. Similar statistics are found around the world [19, 25]. Roads are likely get busier day-by-day with the increasing human population and number of vehicles. Recent vehicles are being equipped with GPS and Wi-Fi devices that enable vehicle-to-vehicle (V2V) communications, forming a VANETs. Using these devices, VANETs can help improve road safety and traffic efficiency by exchanging information among vehicles and is envisioned to be an important application with enormous societal impact. VANETs have attracted both academia and industries [14, 19, 25] such as the Car to Car Communication Consortium [4] as well as projects such as NoW [6], PReVENT [7], ORBIT [5], and PATH [3]. These works cover almost all aspect of vehicular communications [14,19,25].

VANET is expected to use a variety of wireless technologies and it can use roadside infrastructure for vehicle-to-roadside (V2R) communications. In V2R based communications, trustworthiness of the message can be easily verified since the locally centralized roadside unit can keep track of the messages and participating vehicles. However, as the message travels from a source vehicle to a destination vehicle through roadside unit, the message might face high delay which might not be tolerable in vehicular communications [26]. In V2V based communications, each vehicle works as a router, destination and source of the message. Therefore, it is challenging for a vehicle to verify whether the recently received message is legitimate or not. In order to address trust and security issues in VANET, there are different approaches proposed in the literature [12, 14, 21, 24, 28, 29] such as location based security [29] sharing safety messages [37], traffic view systems [18], cooperative collision avoidance [11] and so on. Messages in VANETs can be secured using cryptographic algorithms and protocols. Usually a third party, believed as a trust center, is involved in these protocols, e.g., for key distribution, message authentication and digital signatures. However, such mechanism are not attractive solutions in terms of trust as well as economical point of view.

In this paper, we investigate a distributed technique to accomplish automatic detection of malicious vehicle/driver in VANET to get genuine

message in the network. It is noted that if the message is not legitimate, it can be discarded and/or alerted the driver by sending a warning message. Our technique has two approaches: probabilistic and deterministic. In *probabilistic approach*, each vehicle is expected to receive multiple copies of the same message from its peers. The messages from multiple vehicles are used to find the trust levels based on whether the received message has been altered or not. In *deterministic approach*, we consider two different ways to estimate the distance between two communicating vehicles and compare them to verify whether or not the received message is from legitimate vehicle. It is worth noting that the received message might be from nearby road side intruder or false driver on the road. By calculating two distances (based on vehicles' position coordinates and received signal strength) and comparing them help verify the validity of the vehicle and thus the message. In this approach, we consider that the position coordinates are exchanged by vehicles periodically [14, 19] or can be estimated by using existing positioning algorithms [8, 15, 31].

The paper is organized as follows: we present related work in Section 2, trust in VANET and problem statement in Section 3 followed by the proposed approaches and simulation results in Section 4. Section 5 concludes the paper.

2 RELATED WORK

Related work on trust based security management in VANETs can be divided into two categories: centralized-based and distributed-based [13, 16, 17, 20, 27, 30, 34–36, 38, 39]. In centralized based approach, central unit controls the overall VANETs such as in [27, 39] for trust management. In [39], authors have proposed Lightweight Directory Access Protocol (LDAP) directory server-based new certificate revocation mechanism for trust management in which certificate revocation list issued by LDAP directory server can be read in real-time. In [27], authors have proposed a misbehavior detection module for eviction of misbehaving and faulty vehicles to improve the trust in VANETs. In distributed based approaches, VANETs make use of vehicle-to-vehicle interactions to calculate and update trustworthiness of another vehicle such as in [16, 17]). These work consider a single interaction among vehicles for trust management that may have mislead to false alarm. The work presented in [35] uses reputation based privacy preservation in which each vehicle includes signed message group ID and a static group assigned off-line. Group manager plays role in case of disputes or attacks. Similarly in [10], authors have discussed privacy and trust, and proposed centrally assigned digital pseudonyms. Authors in [9] have proposed a method in which vehicles change their pseudonyms in certain region where many vehicles are within

the communication range. This method cannot work in the case when there are not sufficient number of / We note that most of the research and proposed solution in trust based security mainly focus either on the use of pseudonyms and the algorithms changing them or on group leader based control or single parameter and interaction with peers or offline group ID assignment. Implementing pseudonyms in VANET is challenging and applying group leader based V2V communication may introduce higher delay. Furthermore, use of single parameter and interaction with peers may not give accurate trust levels needed in VANETs. In such case, automated and distributed trust management is important while implementing privacy and security. In this work, vehicles measure the trust levels based on more than one methods (parameters and interactions) with peers in which the actual identity of drivers/vehicles are unknown.

3 TRUST IN VANET ENVIRONMENT AND PROBLEM STATEMENT

Trust is an important factor in VANET security that describes a set of relations among communicating vehicles. Trust establishment and maintenance for fixed infrastructure based wireless communication networks such as cellular systems and Internet, requires a lengthy process but it is assumed to be validated for long time. For such infrastructure based wireless system assuming that base stations in cellular systems or access points in Wireless LAN trust are high, existing approaches to trust management can be applied with minor modification straightforwardly as at least the roadside infrastructure is stationary. In contrast, frequent changing topology and network life-time in VANETs make trust management a challenging problem and requires considerable attention. When vehicles are within the communicating range with others, they start interacting with each other. In VANETs, each vehicle may not be able to detect an incident since a vehicle might be looking for traffic updates which might be miles of distance away from the incident area. In such scenario, vehicle has to rely on the information received from other vehicles. Without having proper mechanism for trust management, communication in VANET might be prone to security threat. Generally, VANET security system should protect the privacy of both drivers and passengers [29] however it should be able to help establish the liability of drivers. It is worth noting that the key element in VANET security is *trust* that prevents generic attack on the network. Thus, the verification of a message received from other vehicles are required to protect the network from malicious drivers. As we know the information of vehicle is linked with personal information (of owner or renter), and thus it is required to protect personal information from being

disclosed to unauthorized users for their privacy. A vehicle can collect the messages from any vehicles but the vehicle might not be able to verify whether the message is legitimate. Privacy level of VANETs after implementing wireless communications should be at least with the same level which is obtained without implementing wireless communications [33]. Specific privacy threats in VANETs are: tracking a specific vehicle, cheating with information, and so on. The general principle of privacy in VANETs is to protect the participating drivers/vehicles against the non-authorized users however it should be disclosable to authorized parties. Use of actual identity of vehicle or owner can easily be vulnerable to privacy. It is important to verify that the received information in VANETs is coming from trustworthy peers. Each vehicle should be able to evaluate, decide and react locally on information received from other vehicles without violating privacy of vehicles or owners.

Our goal in this paper is to cast a problem for trust-based VANET security using probabilistic and deterministic approaches which are based on the local information obtained through interactions among vehicles to determine legitimacy of the messages and to decide whether the messages would be considered for further transmission over the VANET or be dropped.

4 PROPOSED APPROACH

We present an analysis for malicious driver detection through trust of the received message using probabilistic approach and deterministic approach in the following sections.

4.1 Probabilistic Approach

In this probabilistic approach, we consider that $X_i(t)$ is the message transmitted by a vehicle i in VANETs at time slot t. A given vehicle i will attack the VANET with probability p_a by sending the information $X_i(t) \pm \delta$. It is worth noting that the message $X_i(t) \pm \delta$ represents the modified message since δ message is added or removed from the original message.

We also consider that there will be no change in message when instantaneous signal-to-noise-ratio (SNR), γ_i, is greater than its SNR threshold, $\overline{\gamma}_i$, and the probability of error (because of lower instantaneous SNR than the given threshold) can be computed as

$$P_{i,snr} = Pr\{\gamma_i < \overline{\gamma}_i\} = 1 - Pr\{\gamma_i \geq \overline{\gamma}_i\} \tag{1}$$

Single Malicious Driver Detection

We consider that there is at most one malicious driver in VANETs among participating N vehicles for a given geographic location. Then, we define the

suspicion level of a vehicle/driver i as

$$\pi_i(t) \equiv P(T_i = M|\mathcal{O}_t) \tag{2}$$

where T_i is the type of driver that could be malicious (M) or Honest (H) and $\mathcal{O}_t$ is the observation collected for the interval t (i.e. $[0, t]$). Then, using Bayesian criterion,

$$\pi_i(t) = \frac{P(\mathcal{O}_t|T_i = M)P(T_i = M)}{\sum_{m=1}^{N} P(\mathcal{O}_t|T_m = M)P(T_m = M)} \tag{3}$$

Without loss of generality, we consider that any vehicle can be a malicious with probability $P(T_i = M) = \rho = P(\mathcal{O}_t|T_m = M)$. Then the equation (3) is expressed as [22]

$$\pi_i(t) = \frac{P(\mathcal{O}_t|T_i = M)}{\sum_{m=1}^{N} P(\mathcal{O}_t|T_m = M)} \tag{4}$$

For the denominator part of (4), we can write

$$\begin{aligned}
& P(\mathcal{O}_t|T_i = M) \\
= \;& P(\mathbf{X}(\tau)|T_i = M, \mathcal{O}_{\tau-1})P(\mathcal{O}_{\tau-1}|T_i = M,) \\
= \;& \vdots \\
= \;& \prod_{\tau=1}^{t} P(\mathbf{X}(\tau)|T_i = M, \mathcal{O}_{\tau-1}) \\
= \;& \prod_{\tau=1}^{t} \underbrace{\left[\prod_{j=1, j\neq i}^{N} P(X_j(\tau)|T_j = H)\right] P(X_i(\tau)|\mathcal{O}_{\tau-1})}_{\rho_i(\tau)} \\
= \;& \prod_{\tau=1}^{t} \rho_i(\tau)
\end{aligned} \tag{5}$$

Equation (5) represent the probability of sending message at time slot t conditioned that vehicle i is malicious.

Using equation (4) and (5), the suspicion level $\pi_i(t)$ of the vehicle/driver i can be written as

$$\pi_i(t) = \frac{\prod_{\tau=1}^{t} \rho_i(\tau)}{\sum_{j=1}^{N} \prod_{\tau=1}^{t} \rho_j(\tau)} \tag{6}$$

Equation (6) gives the suspicion level when communication is error free (i.e., when instantaneous SNR is *greater than or equal to* the minimum SNR requirement). However when SNR is considered and the transmission is imperfect (i.e., when instantaneous SNR is *less than* the minimum SNR requirement) because of noise, $\pi_i(t)$, is rewritten as

$$\begin{aligned} \pi_i(t,\gamma_i) &= \pi_i(t) \times P_{i,snr} \\ &= \frac{\prod_{\tau=1}^{t} \rho_i(\tau)}{\sum_{j=1}^{N}\prod_{\tau=1}^{t} \rho_j(\tau)} \times Pr\{\gamma_i < \overline{\gamma}_i\} \end{aligned} \tag{7}$$

It is worth noting that the suspicion level and trust level of a driver are regarded as complement/opposite character, thus the trust level $\hat{\phi}_i(t,\gamma_i)$ of a vehicle/driver i can be computed from its suspicion level $\pi_i(t,\gamma_i)$ as

$$\hat{\phi}_i(t,\gamma_i) = 1 - \pi_i(t,\gamma_i) \tag{8}$$

Note that $\hat{\phi}_i(t,\gamma_i)$ gives trustworthiness of a participating vehicle/driver i.

Based on the analysis presented above, the algorithm is stated as **Algorithm 1**. It is worth noting that the trustworthy message obtained from Algorithm 1 will be transmitted by a vehicle over the VANET and other messages will be disregarded. Note that the threshold in Algorithm 1 can be different for different vehicles and changed on the fly based on its history.

Algorithm 1 Single Malicious Driver Detection

1: **Input**: receive messages from N participating vehicles over the observation period t, and take an initial threshold value λ_T
2: **repeat**
3: compute trust values $\{\hat{\phi}_i(t,\gamma_i)\}_{i=1}^{N}$
4: **for** each vehicle i **do**
5: **if** $\hat{\phi}_i(t,\gamma_i) < \lambda_T$ **then**
6: vehicle/driver i is untrustworthy so the message from i is removed.
7: **else**
8: vehicle/driver i is trustworthy so the message from vehicle i is kept.
9: **end if**
10: **end for**
11: **until** message is received from other vehicles
12: **Output**: trustworthy message or malicious driver i.

Multiple Malicious Drivers Detection

The nature of VANETs is dynamically changing and a vehicle can join a network and leave it at any time according to its destination when it is possible to do so. There might be more than one malicious drivers. Thus, we extend our single malicious driver detection method for multiple malicious drivers.

We consider that the set of malicious drivers $\mathcal{M}$ in VANET which is a subset of all participating vehicles (i.e. $\mathcal{M} \subset \{1, 2, \ldots, N\}$), and define

$$\pi_{\mathcal{M}(t)} \equiv P(T_j = M, \forall j \in \mathcal{M}, T_m = H, \forall m \notin \mathcal{M} | \mathcal{O}_t) \tag{9}$$

It is worth noting that the set $\mathcal{M}$ consists of only malicious drivers while all other drivers are honest and it becomes a NULL set when all drivers are honest. Without loss of generality, we consider that, in the beginning, the set $\mathcal{M}$ is null. For particular set of malicious drivers Θ, we can apply Bayesian criterion as

$$\pi_{\mathcal{M}(t)} = \frac{P(\mathcal{O}_t|\mathcal{M})P(\mathcal{M})}{\sum_{\Theta} P(\mathcal{O}_t|\Theta)P(\Theta)} \tag{10}$$

Without loss of generality, considering that $P(T_j = M) = \rho = P(T_j = \Theta)$ for all drivers and using the similar approach that is used in Section 4.1.1, we can write

$$P(\mathcal{M}) = \rho^{|\mathcal{M}|}(1-\rho)^{N-|\mathcal{M}|} \tag{11}$$

where $|\mathcal{M}|$ is cardinality of the set of malicious drivers $\mathcal{M}$. Now, we can express

$$\begin{aligned} P(\mathcal{O}_t|\mathcal{M}) &= \prod_{\tau=1}^{t} \underbrace{\left[\prod_{j \notin \mathcal{M}} P(X_j(\tau)|T_j = H) \prod_{m \in \mathcal{M}} P(X_m(\tau)|F, \mathcal{O}_{\tau-1}) \right]}_{\rho_{\mathcal{M}}(\tau)} \\ &= \prod_{\tau=1}^{t} \rho_{\mathcal{M}}(\tau) \end{aligned} \tag{12}$$

Using equations (9)−(12), we can calculate the probability that the given set $\mathcal{M}$ contains only malicious drivers. That is, find $\mathcal{M}$ at given time t with largest $\pi_{\mathcal{M}}(t)$ and compare with a given threshold. If it is higher than the given threshold, all the drivers in $\mathcal{M}$ are malicious drivers. When channel

has noise and there is loss in signal, we can write

$$\pi_{\mathcal{M}}(t, \gamma_M) = \pi_{\mathcal{M}}(t)\{P_{i,snr}\}_{\forall i \in \mathcal{M}}$$

Then we can compute trust level $\hat{\phi}_{\mathcal{M}}(t, \gamma_M)$ from suspicion level $\pi_{\mathcal{M}}(t, \gamma_M)$ as

$$\hat{\phi}_{\mathcal{M}}(t, \gamma_M) = 1 - \pi_{\mathcal{M}}(t, \gamma_M) \tag{13}$$

Based on the analysis presented above, the algorithm is stated as **Algorithm 2** which disregards the malicious message for further transmission.

Simulation and Performance Evaluation
To simulate VANETs scenario, we have considered that the rate of vehicles entering to the road segment and exiting from the road segment is same, and

Algorithm 2 Multiple Malicious Driver Detection

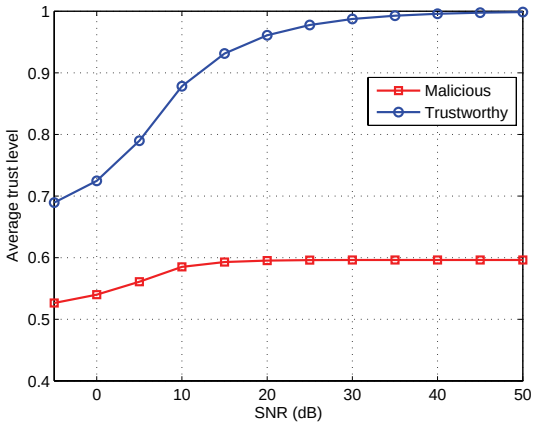
1: **Input**:

- receive messages from N participating vehicles over the observation period t,
- initialize the set of malicious drivers $\mathcal{M} = \{0\}$, and
- take an initial threshold value $\lambda_{\mathcal{M}}$

2: **repeat**
3: Fetch *Algorithm 1* for each vehicle $i \in \{1, \ldots, N\}$ and put a driver in to a malicious set $\mathcal{M}$ if the driver is malicious one according to *Algorithm 1*.
4: **for** each vehicle $i \in \{1, \ldots, N\}$ **do**
5: compute trust values $\hat{\phi}_{\mathcal{M}}(t, \gamma_i)$ using equation (13)
6: **if** $\hat{\phi}_{\mathcal{M}}(t, \gamma_i) < \lambda_{\mathcal{M}}$ **then**
7: the message from a set of drivers $\mathcal{M}$ is removed.
8: **else**
9: Fetch *Algorithm 1* for each vehicle $m \in \{1, \ldots, \mathcal{M}\}$ to check whether a driver m in the set $\mathcal{M}$ is malicious one or not.
If the driver is malicious one according to *Algorithm 1*, then keep him/her in the set $\mathcal{M}$ OTHERWISE remove him/her from the malicious set $\mathcal{M}$.
10: **end if**
11: **end for**
12: **until** message is received from other vehicles
13: **Output**: trustworthy message.

the road segment is chosen to be 10 miles (16093.44 meter) with 4 lane highway. The rate of vehicle entering the road with a given arrival rate $\lambda = 1$ vehicle/sec/lane with average speed of 55 $\pm$10 miles/hour. Noise is assumed to be a Gaussian for signal-to-noise ratio (SNR) levels. Received messages are assumed error free when received SNR is greater than or equal to the minimum/required SNR for a given vehicle. Otherwise, there will be error in received message, and thus the transmitting vehicle will be treated as a malicious one since the receiver vehicle assumes that message is altered by transmitting vehicle. All vehicles use maximum transmission power 35dBm which corresponds to maximum transmission range 1000m in DSRC standard [2, 32]. All vehicles are assumed to be equipped with communication and computing equipment so that each vehicle can communicate with its neighboring vehicles.

In the first experiment, we calculated trust levels based on the received messages for different SNR values. We consider that some vehicles act as malicious ones by changing message while transmitting it to other vehicles. We plotted the average trust value of messages received from vehicles (both genuine and malicious) for different SNR values as shown in Figure 1. Note that, as expected, the trust value increases when SNR increases and reaches to 1 for genuine vehicles. However, the trust levels for untrustworthy drivers remains below 0.65 for all SNR values and are constant even for high SNR values (10dB $-$ 30dB) as shown in Figure 1. When a threshold, $\lambda_T = 0.65$, is chosen, one can easily identify malicious vehicles/drivers. However, the threshold can be adapted dynamically according to the operating environment.



FIGUR E 1
Average trust level of genuine and malicious vehicles/drivers for different SNR values

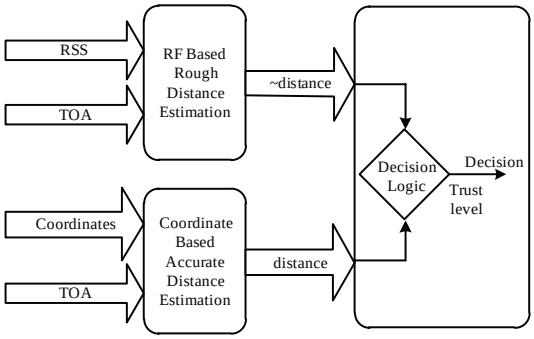


FIGURE 2
Message validation in vehicular ad hoc networks using distances estimated based on RSS and position coordinates

It is important to note that the trust level based on a single instance of a received message might mislead the decision. Thus, we have considered the decision based on an observation period which incorporates the temporary history of the drivers. As the observation time increases, the decision will be more accurate however the time needed to make the decision will be high which might not be suitable for time critical messages. We need to consider some trade-off between the observation time and the time needed to report the decision. Note that probabilistic approach calculates the trust without using any private information of vehicles/owners and thus provides privacy as a byproduct.

4.2 Deterministic Approach for Detecting Malicious Drivers

In this section, we present deterministic approach to measure trustworthiness of the received messages which depends on distances calculated using two different methods as shown in Figure 2. We use the following method to calculate distances and use it to detect legitimacy of the received messages.

Distance Based on Location Coordinate

We note that according to the DSRC standard [2, 32] every vehicle broadcasts/reports its periodic information 10 times every second through control channel so that nearby other vehicles know its position. The periodic information in VANETs contains the location of the vehicle. We consider that (x_0, y_0, z_0) is the x, y and z coordinates of a vehicle who receives the message and $(x_1^{(i)}, y_1^{(i)}, z_1^{(i)})$ is the corresponding x, y and z coordinates of a given vehicle i who transmits the information. In this case z takes care of the altitude when a vehicle is at multistory building or is traveling on flyover structures. Based on location coordinates, for a given vehicle i, distance between

two communicating vehicles at given time instance n can be calculated using following equation

$$d_c^{(i)}(n) = \sqrt{(x_0 - x_1^{(i)})^2 + (y_0 - y_1^{(i)})^2 + (z_0 - z_1^{(i)})^2} \tag{14}$$

Using this equation, the distance between any two vehicles can be computed. In order to increase the accuracy of distance calculations, time of arrival (TOA) is also taken into account.

Distance Based on Received Signal Strength (RSS)

According to the DSRC standard [2, 32], the maximum transmit power level of each vehicle is predefined. For a given transmit power level, measuring the RSS or received power, distance between two vehicles can be calculated [23]. It is worth noting that the received power measurement should not be done based on periodic broadcast messages. It is noted that, for given transmit power $p_t^{(i)}$, the received power $p_r^{(i)}$ can be calculated as [23]

$$p_r^{(i)} = p_t^{(i)} G_t^{(i)} G_r^{(i)} \frac{h_t^{(i)2} h_r^{(i)2}}{d_p^{(i)4} L^{(i)}} \tag{15}$$

where $h_t^{(i)}$ and $h_r^{(i)}$ are respectively height of transmit and receive antenna, $G_t^{(i)}$ and $G_r^{(i)}$ are respectively transmit and receive antenna gain, $L^{(i)}$ is system loss factor and $d_p^{(i)}$ is the distance between a transmitter vehicle and a given receiver vehicle i.

Without loss of generality, we consider $h_t^{(i)}$, $h_r^{(i)}$, $G_t^{(i)}$, and G_r constant and equal to unity. We note that the system loss factor $L^{(i)}$ is constant for given environment* , and the equation (15) can be expressed as

$$p_r^{(i)} = \frac{p_t^{(i)}}{d_p^{(i)4}} \tag{16}$$

where the received power level depends only on transmit power $p_t^{(i)}$ and distance $d_p^{(i)}$. Thus, for given transmit power (which is constant according to DSRC in this case), the distance $d_p^{(i)}$, for a given vehicle i at given time instance n, is given by

$$d_p^{(i)}(n) = \left(\frac{p_t^{(i)}}{p_r^{(i)}} \right)^{\frac{1}{4}} \tag{17}$$

* Based on the posted speed limit of the road which can be obtained with the help of GPS systems, the value of $L^{(i)}$ can be incorporated for the distance calculation. High speed limit and low/city speed limits imply that the communication environment are, respectively, rural and urban/city.

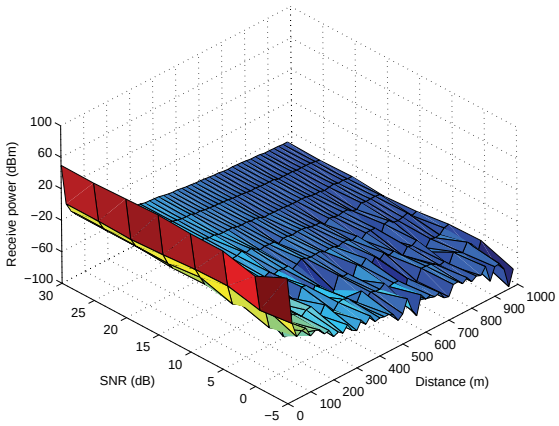


FIGURE 3
Variation of received signal power for different SNRs and distances between transmitter and receiver vehicles.

By using equation (17), the distance between two vehicles can be estimated based on the received power level provided that the transmit power $p_t^{(i)}$ is known. As mentioned previously, time of arrival of the message is also considered to increase the accuracy of estimation.

We have simulated the scenario to find received power level for a given transmit power and distances used in DSRC enabled vehicles. Figure 3 shows the variation of received power for different SNRs and increasing distance between transmitter and receiver vehicles. As expected the received power fluctuation is higher in the case of low SNR value than that with high SNR. Furthermore, as the distance increases, the received power level decreases.

It is important to note that, based on the periodic status message and with the help of speed and time information, the distances $d_p^{(i)}(n)$ and $d_c^{(i)}(n)$ can be synchronized or estimated for new time instance if these two distances are evaluated for different TOAs.

Measuring Trustworthiness Using Distances Calculated Two Different Approaches

The distances $d_c^{(i)}$ and $d_p^{(i)}$ should be equal (ideally this difference should be equal to zero) for given vehicles if the transmitting vehicle is a legitimate one. In VANETs, the location estimation might have some errors because of high speed of vehicles. Thus we consider that the transmitting vehicle is a legitimate one when difference between $d_c^{(i)}$ and $d_p^{(i)}$ is within the tolerable

limit ϵ and the difference is given by

$$D_i(n) = |d_c^{(i)}(n) - d_p^{(i)}(n)| \tag{18}$$

When the difference D_i at time n is less than tolerance ϵ[†], we assume that two distances are equal otherwise the distances do not belong to the same vehicle. That is, when the condition $D_i(n) < \epsilon$ satisfies, a vehicle assumes that the communication is with legitimate vehicles. Otherwise it is assumed that the vehicle is communicating with malicious ones. There are apparent chances of being more than one transmit vehicles at equidistant from a receiver vehicle because of estimation errors, which results in probability of false alarm p_{fa}. The false alarm probability, p_{fa}, can be expressed as

$$\begin{aligned} p_{fa} &= P(D_i < \epsilon | v_i \text{ was not at } (x_1^{(i)}, y_1^{(i)}, z_1^{(i)})) \\ &+ P(D_i > \epsilon | v_i \text{ was at } (x_1^{(i)}, y_1^{(i)}, z_1^{(i)})) \end{aligned} \tag{19}$$

Based on the calculated distances, we define a suspicion level for a vehicle i as

$$\psi_i = \min\{1, \frac{D_i}{d_c^{(i)}}\} \tag{20}$$

When we consider noise transmission, the suspicion level becomes

$$\bar{\psi}_i = \psi_i \times P_{i,snr} = \psi_i \times Pr\{\gamma_i < \overline{\gamma}_i\} \tag{21}$$

and the trust level of the vehicle i as

$$\bar{\phi}_i = 1 - \bar{\psi}_i \tag{22}$$

It is noted that the trust level $\bar{\phi}_i$ in the equation (22) is 1 when $D_i = 0$ that is when the estimated distances using two different approaches are exactly equal. The trust level cannot be greater than one and less than zero. Then total trust level for N participating vehicles is defined as

$$\bar{\Phi}_t = \sum_{j=1}^{N} e^{\bar{\phi}_j^k}(A_j \times B_j) \tag{23}$$

[†] In this case the value of ϵ is considered to be as short as the size of a normal car since two communicating vehicles cannot have same position (or coordinates) for given time in normal conditions.

Where k is penalty factor and

$$\begin{array}{ll} A_j = -1 & \text{for}\{D_i < \epsilon |\ v_i \text{ wasn't at } (x_1^{(i)}, y_1^{(i)}, z_1^{(i)})\} \\ A_j = 1 & \text{otherwise} \end{array}$$

and

$$B_j = -1 \text{ for } \{D_i > \epsilon | v_i \text{ was at } (x_1^{(i)}, y_1^{(i)}, z_1^{(i)})\}$$

$$\text{and } \{D_i > \epsilon | v_i \text{ wasn't at } (x_1^{(i)}, y_1^{(i)}, z_1^{(i)})\}$$

$$B_j = 1 \quad \text{otherwise}$$

Based on this, we can define two hypotheses as

$$\begin{array}{lll} \mathcal{H}_0 & : & \bar{\Phi}_t = -\sum_{j=1}^{N} e^{\bar{\phi}_j^k}, \text{ for } A_j \times B_j = -1, \forall j \\ \mathcal{H}_1 & : & \bar{\Phi}_t = \sum_{j=1}^{N} e^{\bar{\phi}_j^k}, \text{ for } A_j \times B_j = +1, \forall j \end{array} \tag{24}$$

For instance, in Figure 4, the vehicle v_0 on the road computes its distance to all other communicating vehicles. For an instance, vehicle v_0 will know coordinates of other participating vehicles through periodic broadcast messages, and the distances from a vehicle v_0 to other vehicles v_1, v_2 and v_3 for given/known coordinates using equation (14) which are respectively $d_c^{(i=1)} = 166.43$, $d_c^{(i=2)} = 85.00$ and $d_c^{(i=3)} = 49.24$. Once a vehicle v_0 gets actual message from other vehicle (say from vehicle v_1), it computes the distance $d_p^{(i=1)}$ between a transmitter vehicle v_1 and v_0 using equation (17), and the computed value $d_p^{(i=1)}$ at a given time is compared with corresponding distance $d_c^{(i=1)}$, and then checks the validity of the received message. It is noted that, in an ideal case, $d_p^{(i=1)} = d_c^{(i=1)}$ for a given time instance. For

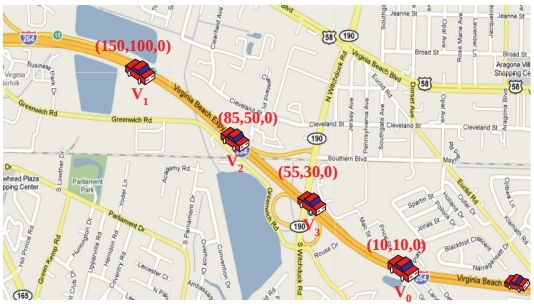


FIGURE 4
Five vehicles, traveling on highway, are shown with their corresponding position coordinates and the vehicle V_0 estimates its distance from all other transmitter vehicles who are in front of it.

Algorithm 3 Trustworthy calculation

Input: Initial transmit power p_t and the tolerance ϵ.
for all vehicles **do**
  while message is received **do**
    Determine the distance $d_c^{(i)}$ using equation (14).
    Determine the distance $d_p^{(i)}$ using equation (17).
    Compute D_i using equation (18).
    if $D_i > \epsilon$ **then**
    Discard the received message from vehicle i.
    else
    The received message is trustworthy one.
    end if
    Calculate the trust level using equation (23).
  end while
end for
Output: Legitimate message and trust level.

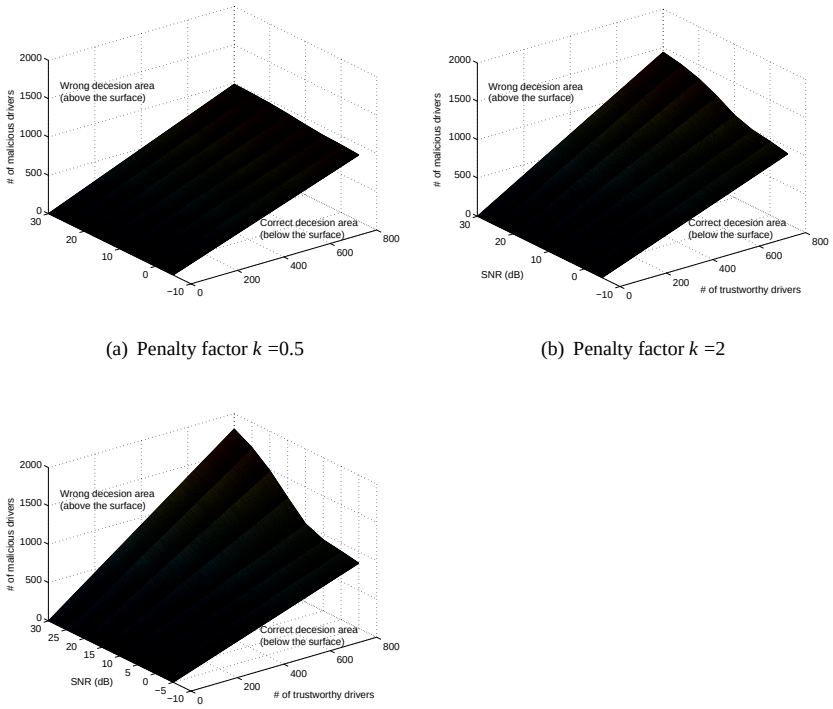
example, based on RSS, the distance between vehicle v_0 and v_1 is $d_p^{(i=1)} = 110.20$ (say). Then vehicle v_0 discards the message received from vehicle v_1 since the difference $D_{i=1} = 56.23$ that is greater than the tolerance $\epsilon = 10$. The suspicion level in this case is 33.79% and trust level is 66.21%.

Similarly, if v_0 receives actual message from v_2 same process will be repeated. When estimated distances for more than one vehicle are equal, the given vehicle uses the coordinates or direction information embedded in regular status broadcast information to find the vehicles' location in addition to two distances. We note that a vehicle knows the position or traveling lane or travel direction of the communicating vehicle with the help of their regular broadcast status information and position coordinates. We also consider that the vehicle can neglect the message received from the vehicles which are behind a given vehicle since the message might not carry any relevant information for upcoming traffic needed to the given vehicle. Note that when the calculated distances from a receiver vehicle to other many vehicles are equal, there will be false alarm.

Based on the analysis presented above, the algorithm is stated as **Algorithm 3**. If the message is legitimate, a vehicle forwards it to other vehicles. Otherwise, the message is disregarded.

Simulation and Performance Evaluation

As mentioned, each vehicle exchanges its status with its neighboring vehicles approximately 10 times each second [2], and thus the distance between



(a) Penalty factor k =0.5

(b) Penalty factor k =2

(c) Penalty factor k=5

FIGURE 5
Trust metric for different penalty factors with wrong and correct decision region. Correct decision region increases with the increasing penalty factor.

vehicles is calculated based on the location coordinates. We have also considered that, as the given vehicle receives a regular message, it also calculates its distance from transmitting vehicle based on the RSS using Algorithm 3.

In the next experiment, we have computed trust level of the received message using **Algorithm 3** so that they can filter out the message received from malicious vehicles/drivers to prevent VANETs from malicious actions. Figure 5 (a), (b), and (c) show that the correct decision region increases (equivalently wrong decision region decreases) with increase in penalty factor k. It is noted that, as expected, the correct decision region increases with the increase in SNR values as shown in Figure 5 (a), (b), and (c).

4.3 Combining Probabilistic and Deterministic Approaches

In this section, we compare pure probabilistic, deterministic, and combined (deterministic followed by a probabilistic) approaches. In this scenario, each

Algorithm 4 Combined approach

1: **Input**: Message from peers
2: **repeat**
3: **for** each vehicle i **do**
4: Decide whether the distances are within the tolerance level as shown in Figure 2
5: **if** vehicle is legitimate (i.e. $D_i < \epsilon$) **then** Apply probabilistic approach as mentioned in Algorithm 2.
6: **else**
7: Discard the message received from vehicle i.
8: **end if**
9: **end for**
10: **until** message is received from other peers
11: **Output**: trust level, trustworthy message or malicious driver i.

vehicle apply the deterministic approach to check whether or not the distance difference D_i is within the given tolerance. If communicating peers are within the tolerance limit, then vehicle applies probabilistic approaches as given in **Algorithm 4**.

As shown in Figure 6, we note that the combined approach is the best among all as it filters the message using both probabilistic and deterministic approaches. However, as expected, the time required to make decision is the highest in combined method and the least in the case of deterministic approach as shown in Figure 7. Note that the probabilistic approach takes

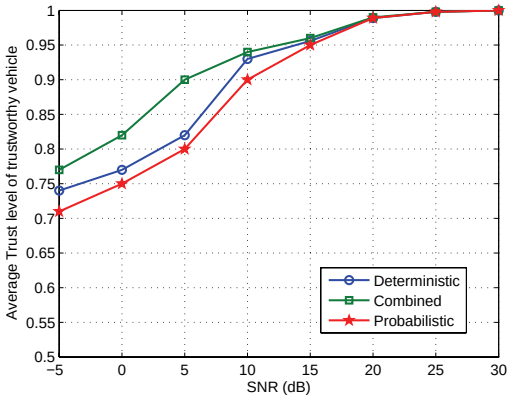


FIGURE 6
Comparison of average trust level for different SNR values for trustworthy vehicles

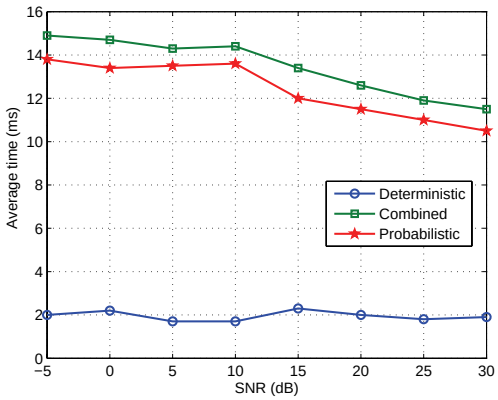
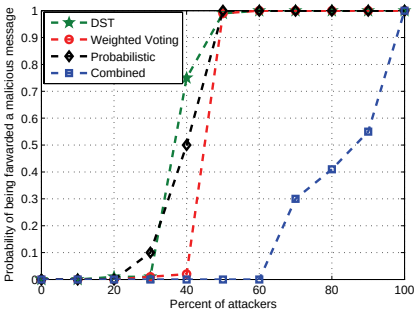


FIGURE 7
Comparison of average time required to make a decision by a vehicle for different SNR values for trustworthy vehicles. The average observation time for probabilistic approach was set to 12 ms.

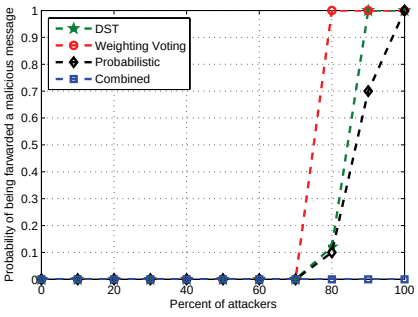
some observation time to make a decision as a result it takes more time than that of deterministic approach.

We conclude that the combined method gives higher trust level for low SNRs but needs more time to make a decision. The deterministic approach is the best in terms of time needed to make a decision however there might be error in coordinate estimation, and the RSS might be highly faded which may result in inaccurate decision that might mislead the communication in VANETs.

Finally, we compare the performance of the proposed approaches (both probabilistic and deterministic) with the weighted majority voting [20, 30] and Dempster-Shafer Theory (DST) [34] in terms of probability of forwarding a malicious message for different percentage of attackers as shown in Figures 8 (a) and (b). Note that the attackers are those who change messages partially or completely and/or report their geolocation coordinates incorrectly. In Figures 8 (a) and (b), we observe that the combined (proposed) approach gives better results since the trust level is calculated combining two different methods. The proposed probabilistic approach alone gives better result than the methods in the state-of-the-art [20, 30, 34] when the trust levels of malicious vehicles are lower than the cutoff trust level as shown in Figure 8(b). Whereas the probabilistic approach gives comparable results with the state-of-the-art work when the trust levels of malicious vehicles are lower than the cutoff trust level as shown in Figure 8(a). Note that the proposed combined method gives the best result however it takes more time to make a decision as shown in Figure 7.



(a) Average trust level of attackers (0.8) is higher than the cutoff trust level 0.6



(b) Average trust level of attackers (0.3) is lower than the cutoff trust level 0.6

FIGURE 8
Performance comparison of proposed schemes (probabilistic and combined) with the weighted voting [20, 30] and Dempster-Shafer Theory (DST) [34] for different percentage of attackers.

5 CONCLUSION

In this paper, we have proposed probabilistic and deterministic approaches to determine the trust level which is used to filter out malicious information to provide VANET security. In the proposed schemes individual vehicles evaluate, decide and react locally based on the information received from other vehicles. Proposed algorithms determine whether or not the received message is legitimate. Probabilistic approach uses the copies of received message to estimate trust level. Deterministic approach estimates the trust level of the received message by using distances calculated using received signal strength (RSS) with time of arrival (TOA) and vehicle's signal strength (RSS) with time of arrival (TOA) and vehicle's geolocation (position coordinates) along with TOA. We have also investigated the effect of combined approach

(by combining probabilistic and deterministic approaches) for filtering our the message. Using proposed approaches, individual vehicles determine trust level which is used to decide whether the message would be considered for further transmission over the VANET or dropped without any further consideration. We also noted that the penalty factor helps to control the action of malicious users. Combined approach gives better results than the deterministic and probabilistic approaches individually however combined approach needs more time to make a decision. We have validated our claims with the help of results obtained from extensive simulations. As part of the ongoing research, we plan to develop a prototype/testbed of the proposed approach and compare performance results with simulation observations.

ACKNOWLEDGMENTS

The authors are grateful to the anonymous reviewers for their constructive comments on the paper. This work is supported in part by the CEIT-FRSG program at GSU. Preliminary version of this work was presented in part at the 5th International Conference on Complex, Intelligent, and Software Intensive Systems.

REFERENCES

[1] National Highway Traffic Safety Administration 2012 Report. http://www.nhtsa.gov/staticfiles/administration/pdf/Budgets/FY2012_Budget_Overviewv3.pdf.

[2] Vehicle Safety Communications Project Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC. Vehicle Safety Communications Consortium consisting of BMW, Daimler-Chrysler, Ford, GM, Nissian, Toyota, and VW.

[3] (2010). California Partners for Advanced Transit and Highways (PATH). http://www.path.berkeley.edu/.

[4] (2010). Car to Car Communication Consortium (C2CCC). http://www.car-to-car.org/.

[5] (2010). DISCO Lab. http://discolab.rutgers.edu/traffic.

[6] (2010). Network on Wheels (NoW). http://www.network-onwheels.de/.

[7] (2010). PREVENT project. http://www.prevent-ip.org.

[8] P. Bahl and V. Padmanabhan. (2000). RADAR: An in-building RF-based user location and tracking system. In *IEEE INFOCOM*, volume 2, pages 775–784.

[9] A. R. Beresford and F. Stajano. (2004). Mix Zones: User Privacy in Location-aware Services. In *PERCOMW 2004*, page 127, Washington, DC, USA.

[10] F. Dotzer. (2005). Privacy Issues in Vehicular Ad hoc Networks. In *Privacy Enhancing Technologies*, pages 197–209.

[11] T. ElBatt, S.K. Goel, G. Holland, H. Krishnan, and J. Parikh. (2006). Cooperative collision warning using dedicated short range wireless communications. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 1–9.

[12] M. Gerlach, A. Festag, T. Leinmuller, G. Goldacker, and C. Harsch. (2005). Security Architecture for Vehicular Communication. *WIT 2005*.

[13] Félix Gómez Mármol and Gregorio Martínez Pérez. (2012). Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35(3):934–941.

[14] Hannes Hartenstein and Kenneth Laberteaux, editors. (March 2010). *VANET: Vehicular Applications and Inter-Networking Technologies*. John Wiley and Sons.

[15] T. He, C. Huang, B.M. Blum, J.A. Stankovic, and T. Abdelzaher. (2003). Range-free localization schemes for large scale sensor networks. In *Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 81–95.

[16] U.F. Minhas, Jie Zhang, T. Tran, and R. Cohen. (2010). Intelligent Agents in Mobile Vehicular Ad Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty. In *Proceedings of the 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI IAT)*, pages 243–247.

[17] Umar Minhas, Jie Zhang, Thomas Tran, and Robin Cohen. (June 2010). Towards Expanded Trust Management for Agents in Vehicular Ad-hoc Networks. *In International Journal of Computational Intelligence: Theory and Practice (IJCITP)*, pages 3–15.

[18] Tamer Nadeem, Sasan Dashtinezhad, Chunyuan Liao, and Liviu Iftode. (2004). Trafficview: Traffic data dissemination using car-to-car communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 8.

[19] Stephan Olariu and Michele C. Weigle, editors. (March 2009). *Vehicular Networks: From Theory to Practice*. CRC Press / Taylor & Francis.

[20] Benedikt Ostermaier, Florian Dotzer, and Markus Strassberger. (2007). Enhancing the security of local danger warnings in VANETs-a simulative analysis of voting schemes. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pages 422–431.

[21] P. Papadimitratos, V. Gligor, and J.P. Hubaux. (2006). Securing Vehicular Communications-Assumptions, Requirements, and Principles. In *Workshop on Embedded Security in Cars*.

[22] Athanasios Papoulis and S Uikrisha Pillai. (2001). *Probability, random variables and stochastic processes with errata sheet*. McGraw-Hill Science/Engineering/Math.

[23] T.S. Rappaport. (2002). *Wireless Communications: Principles and Practice*. Prentice Hall PTR New Jersey.

[24] D. B. Rawat, B. B. Bista, G. Yan, and M. C. Weigle. (June 2011). Securing Vehicular Ad-Hoc Networks Against Malicious Drivers: A Probabilistic Approach. In *Proceedings of the 5th International Conference on Complex, Intelligent, and Software Intensive Systems*.

[25] D. B. Rawat and G. Yan. *Infrastructures in Vehicular Communications: Status, Challenges and Perspectives*. Dr. M. Watfa, Eds. IGI Global, 2010.

[26] Danda B. Rawat, Dimitrie C. Popescu, Gongjun Yan, and Stephan Olariu. (September 2011). Enhancing VANET Performance by Joint Adaptation of Transmission Power and Contention Window Size. *IEEE Transactions on Parallel and Distributed Systems*, 22(9):1528–1535.

[27] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux. (2007). Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, 25(8):1557–1568.

[28] M. Raya, P. Papadimitratos, J.P. Hubaux, and E.P.F. de Lausanne. (2006). Securing Vehicular Communications. *IEEE Wireless Communications*, 13(5):8–15.

[29] Maxim Raya and Jean-Pierre Hubaux. (2005). The Security of Vehicular Ad hoc Networks. In *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21, New York, NY, USA. ACM.

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

[31] P. Rong and M.L. Sichitiu. (2007). Angle of arrival localization for wireless sensor networks. In *Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual IEEE Communications Society on*, volume 1, pages 374–382.

[32] Raja Sengupta and Qing Xu. (2004). DSRC for Safety Systems. volume 10, pages 2–5. California PATH – Partners for Advanced Transit and Highways.

[33] J. Serna, J. Luna, and M. Medina. (2008). Geolocation-Based Trust for Vanet's Privacy. In *4th International Conference on Information Assurance and Security, ISIAS'08*, pages 287–290.

[34] Glenn Shafer. (1976). *A mathematical theory of evidence*, volume 1. Princeton university press Princeton.

[35] A Tajeddine, A. Kayssi, and A. Chehab. (2010). A Privacy-Preserving Trust Model for VANETs. In *Proceedings of the 2010 IEEE 10th International Conference on Computer and Information Technology (CIT)*, pages 832–837.

[36] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi. (2008). Trust Issues for Vehicular Ad Hoc Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Spring 2008)*, pages 2800–2804.

[37] Q. Xu, T. Mak, J. Ko, and R. Sengupta. (2004). Vehicle-to-vehicle safety messaging in dsrc. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 19–28.

[38] Jie Zhang. (2011). A Survey on Trust Management for VANETs. In *Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pages 105–112.

[39] Shaomin Zhang and Haijiao Wang. (2008). An Improved Delta and Over-issued Certificate Revocation Mechanism. In *Proceedings of the 2008 ISECS International Colloquium on Computing, Communication, Control, and Management*, pages 346–350.