Trust Management Method for Vehicular Ad Hoc Networks

Riaz Ahmed Shaikh and Ahmed Saeed Alzahrani

King Abdulaziz University, Jeddah, Saudi Arabia
{rashaikh,asalzahrani}@kau.edu.sa

Abstract. In vehicular ad hoc networks, evaluating trustworthiness of data is utmost necessary for the receiver to make reliable decisions that are very crucial in safety and traffic-efficiency related applications. Existing trust management schemes that have been proposed so far for the vehicular networks has suffered from various limitations. For example, some schemes build trust based on the history of interactions. However, vehicular networks are ephemeral in nature, which makes that approach infeasible. Furthermore, in most of the existing approaches, unique identities of each vehicle must be known. This violates user privacy. In order to overcome these limitations, we have proposed a novel trust management scheme for the vehicular networks. The proposed method is simple and completely decentralized, which makes it easy to implement in the vehicular networks. We have analytically proved its robustness with respect to various security threats. Furthermore, it introduces linear time complexity, which makes it suitable to use in real-time.

Keywords: Ad-Hoc networks, Privacy, Trust model, Vehicular networks.

1 Introduction

In the last decade, we have witnessed a large increase in research and development in the domain of a vehicular ad hoc networks (VANETs). In the USA, the Federal Communications Commission (FCC) has already allocated 75 MHz of a Dedicated Short Range Communications (DSRC) spectrum at 5.9 GHz band to support vehicular networking [1]. Also, in August 2008, the European Telecommunications Standards Institute (ETSI) has allocated 30 MHz of spectrum in the 5.9 GHz band for vehicular networking [2]. Allocation of a wide DSRC spectrum enables a great number of potential applications including safety applications, real-time traffic management, on-board entertainment and mobile Internet access [3]. Many applications are proposed so far, e.g., General Motors (GM)'s collision warning system [4], Inter-vehicle hazard warning system [5], and Traffic view system [6]. However, most of the focus has been placed on reliable delivery of messages among vehicles, and less focus has been placed on evaluating the reliability of the data sent by the peers [7,8]. This motivates us to work in this direction. We firmly believe that the evaluating quality and reliability of the data is utmost necessary for the receiver to make reliable decisions, which are

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 801–815, 2013.

very crucial in safety and traffic efficiency related applications. For example, a malicious peer wants to create congestion on the road to achieve some criminal goal. For this, he reports the roads on his path as slippery. In the absence of data reliability mechanism, other peers would slow down, thus creating congestion.

Cryptographic-based security solutions do not provide any guarantee or assurance of the quality or reliability of the data itself [9,10]. That can be evaluated by measuring a trust on the sender, where trust is defined as "confidence in or reliance on some quality or attribute of a person or thing, or the truth in a statement" (Oxford English Dictionary, p. 432). The trust level will help to distinguish trusted, malicious, faulty and selfish senders. Only a few trust models have been proposed for the VANETs, e.g., [11,12,13,14,8,15], which has suffered from various limitations that are discussed in the related work section.

Trust management in the VANETs is more complex than the trust management in other networks like sensor networks, MANETs etc., because of the following reasons:

- Nodes move at very high speed, in which time to react to an imminent situation is very critical [7]. Therefore, nodes in the VANETs should be able to evaluate trust in real-time.
- Nodes in the VANETs remains in contact with each other for a short period of time, which may not be enough to establish trust based on reputation or history of interactions [16]. Therefore, trust management schemes in the VANETs should be able to cope with this time scarcity problem.

In this work, we have proposed a novel trust management scheme for the vehicular networks that efficiently deals with the above-mentioned challenges. In addition to that our proposed method has the following properties:

- *Privacy assurance*: Proposed method operates in identity anonymous environment, which ensures identity and location privacy of the user.
- *Distributed trust establishement*: Proposed trust management scheme is completely decentralized, which makes it easy to implement in the VANETs.
- *Robustness*: Proposed method is resilient against attacks on the trust model itself.

Our proposed method works in three phases. In the first phase, receiver nodes will calculate their confidence value on each message that comes from unique senders about a particular event. It is calculated based on three parameters: 1) location closeness, 2) time closeness, and 3) location verification. In the second phase, method will calculate the trust value for each unique message related to the same event. In the last phase, receiver will take the decision of an acceptance of the message, which has the highest trust value.

The rest of this paper is organized as follows: Section 2 contains related work. Section 3 describes the proposed trust management method. Section 4 consists of analysis and evaluation of the proposed method from the perspective of security resiliency and time complexity. Finally, Section 5 concludes the paper and highlights some future work.

2 Related Work

F. G. Mármol and G. M. Pérez [15] have proposed a trust and reputation infrastructure-base proposal (TRIP) for the vehicular ad hoc networks. In that work, the reputation of a node is first calculated based on the three factors: 1) direct previous experiences with the target node, 2) recommendations from other surrounding vehicles, and 3) recommendation from central authority through RSU. After that, system will map the reputation score with one of the three trust levels (1. Trust, 2. Not Trust, and 3. +/- Trust), which are represented as fuzzy sets. The proposed scheme is based on one very strong assumption that is; a vehicle usually circulate over the same road, and at the same time of the day. This will help to built history. We argue that this assumption is not realistic. Furthermore, in order to build a history and reputation, actual identities of vehicles must be known. However, in order to ensure privacy in vehicular-to-vehicular (V2V) communication, the use of temporal pseudo-identities is recommended [7,17].

D. Huang *et al.* [12] have proposed a Situation-Aware Trust (SAT) architecture for the vehicular networks. The SAT includes three main components:

- An attribute-based policy control module, which is used to address a number of trust situations and application scenarios on road,
- Proactive trust module, which is used to build inter-vehicle trust in a timely fashion, and
- An email-based social network trust module, which is used to enhance trust and to allow the set up of a decentralized trust framework.

The SAT requires deployment of both global and local trust agents that makes it hybrid architecture. Authors have suggested various parameters and high level mechanisms that can be used to compute trust. However, they did not provide mathematical model that could show how to combine the various parameters together. Furthermore, authors have suggested the use of email addresses and social networks to compute trust that violates the identity and location privacy of a user.

M. Raya *et al.* [11] have proposed a data-centric trust establishment method for the ephemeral ad hoc networks. In their model, they evaluate trustworthiness of the data reports instead of the trustworthiness of the sender entities themselves. They define various trust matrices, such as, a priori trust relationship (default trustworthiness), event or task-specific trustworthiness, and time and location closeness. They evaluate data reports with corresponding trust metrics using several decision logics, such as weighted voting, Bayesian inference, and Dempster-Shafer Theory. This scheme is suitable only in a scenario, when enough evidence (either in support or against a specific event) is available [7].

U. F. Minhas *et al.* [13] have proposed an expanded trust model for agents in the VANETs. In their model, they have incorporated role-based trust and experience-based trust, that are both combined into the priority-based model which can be used to choose proper advisers. After that, they use majority-opinion approach to aggregate feedback from selected advisers. During feedback aggregation, they also consider time and location closeness factors. In their

model, they assume that roles are pre-defined by the authorities, and are expected to behave in a certain way. Furthermore, robustness has not been extensively addressed [7].

A. Patwardhan *et al.* [14] have proposed a data intensive reputation management scheme for the VANETs. In their model, they use persistent identities, frequency of encounters, and a known set of trustworthy anchored sources to serve as nucleating points for building trust relationships with previously unknown devices. Data is considered to be trustworthy, when there is an agreement among peers (majority consensus) or when it comes from the trustworthy source. During determining the majority consensus, their model does not consider reputation of the peers. Furthermore, authors assumed that each mobile device must have unique persistent identity that violates identity privacy.

C. Chen *et al.* [8] have proposed a trust modelling framework for message propagation and evaluation in the VANETs. In order to model quality of information shared by peers and the trust relationships between peers, they used trust opinions, experience-based trust and role-based trust metrics. Their trust model is binary (either fully trusted or not trusted). Inferring binary trust relationship is not always possible specially when we have incomplete information or when we are in uncertain situations. Furthermore, in their model, privacy and robustness has not been extensively addressed.

3 Proposed Method

As shown in the Figure 1, our proposed method works in three phases. In the first phase, receiver node will calculate its confidence value on each message that comes from the unique sender s_n about an event e. In the second phase, it will calculate the trust value for each unique message for an event e. Note that multiple senders can send same message related to a specific event. In the last phase, method will take the decision of an acceptance of a message, which has the highest trust value. Complete details about each phase are given below.

3.1 Confidence Measurement

Confidence shows the receiver's degree of belief on the data as well as the sender. We measure the confidence (C) value based on the following three parameters:

1. Location closeness (L_c),
2. Time closeness (T_c), and
3. Location verification (L_v).

Location Closeness: Location closeness factor determines the closeness of the sender to the reported event. We model the location closeness L_c as:

$$L_c = \begin{cases} 1 - \dfrac{\min(l_s, l_e)}{\max(l_s, l_e)} & \text{if } |l_s - l_e| < \delta l \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

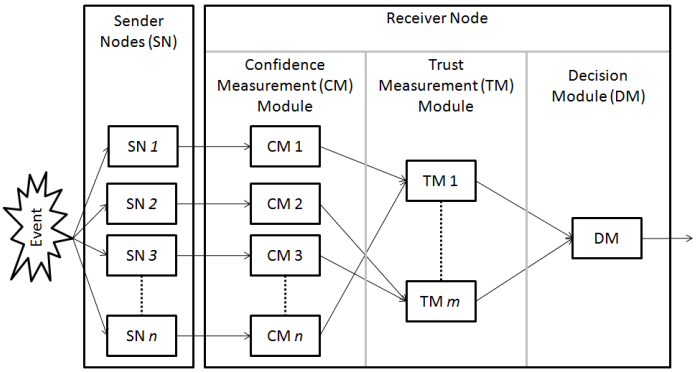


Fig. 1. Proposed Framework

where l_s and l_e represents the location of the source and event respectively. The δl represents a maximum acceptable threshold difference. This location closeness function is developed to keep the following intuitively described requirements.

- Property 1: When the difference between the sender location and event location increases then the location closeness factor also increases.
- Property 2: When the difference between the source location and the event location is more than a pre-defined threshold value then the location closeness factor becomes 1, which means data is not reliable.

The graph in Figure 2 is obtained by implementing the Equation 1 in the Matlab. This graph shows that the location factors increases with the increase in difference between the location of the source and event. This satisfy the property 1. Also, note that when the difference between source and event location is more than the pre-defined threshold value (which in this example is 50 unit), then the location factor becomes 1. This satisfy the property 2.

Time Closeness: Time closeness factor determines the freshness of the data. We model the time closeness T_c as:

$$T_c = \min\left(1, \frac{t_c - t_e}{\delta t}\right) \tag{2}$$

where t_c is the current time and t_e is the event time given in the message; the δt is a threshold time. This time closeness function is developed to keep the following intuitively described requirements.

- Property 1: When the difference between the event time and the current time increases then the time closeness factor also increases.
- Property 2: When the difference between the event time and the current time is more than a pre-defined threshold value then the time closeness factor becomes 1, which means data is outdated.

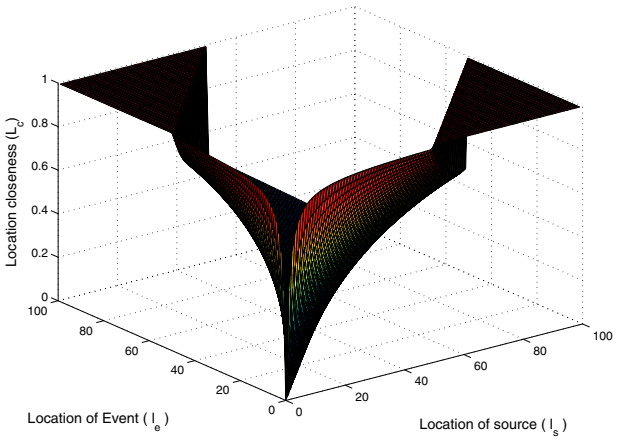


Fig. 2. Analysis of location closeness function: $\delta l = 50$ units

The graph shown in Figure 3 is obtained by implementing the Equation 2. Right side of the graph shows that; with the increase in current time with respect to the event time, the time closeness factor also increases linearly. This satisfy property 1. When current time is greater than 30, the time closeness factor becomes one. This happens because the difference between the current time and event time is more than the threshold value. This satisfy property 2.

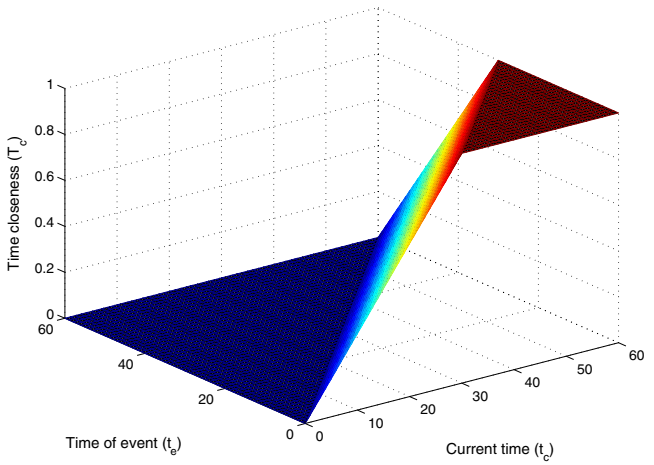


Fig. 3. Analysis of time closeness function: $\delta t = 30$ units

Location Verification: Location verification factor determines whether the sender node has provided its true location or not. Our proposed location verification mechanism (L_v) is described in the Algorithm 1. In this algorithm, first we estimates the region, where the sender is actually located, and then we determines whether the broadcasted coordinates are within the estimated region or not. Detail description of the proposed algorithm is given below.

Let us assume that each vehicle is equipped with a standard embedded device, in such a way that antennas, gains and transmission powers are fixed and known. Let d_{max} is the maximum radio range of the vehicle, and let θ is the angle of arrival of the received packet. How to measure θ is out of the scope of this paper. However, various standard techniques could be employed to measure θ. Whenever a node received a packet, it creates a potential region with the help of θ, and d_{max}, as shown in the Figure 4. Note that receiver's coordinates (x_c, y_c) are reference point. Once the boundaries of possible region are identified (Algo. 1, Lines 2:25), algorithm checks whether the broadcasted coordinates (x_s, y_s) of the sender are within that region or not (Lines 26:30). If (x_s, y_s) are within the identified region, it means the sender has provided true location (Lines 26:27). If (x_s, y_s) are located outside the identified region, it means the sender has provided fake location (Lines 28:29).

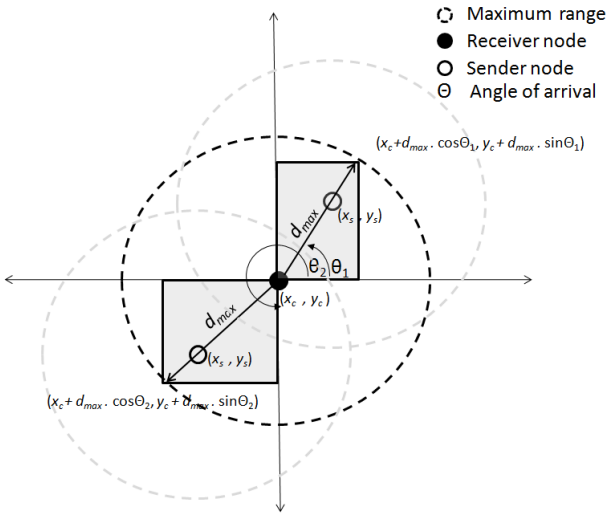


Fig. 4. Region estimation of sender node

Note that, instead of identifying the exact location of the sender, we identify the potential region of the sender. We adopted this approach to achieve simplicity. For better accuracy, other parameters such as signal strength could also be used; however, this will increase the complexity.

Algorithm 1. Location estimation and verification

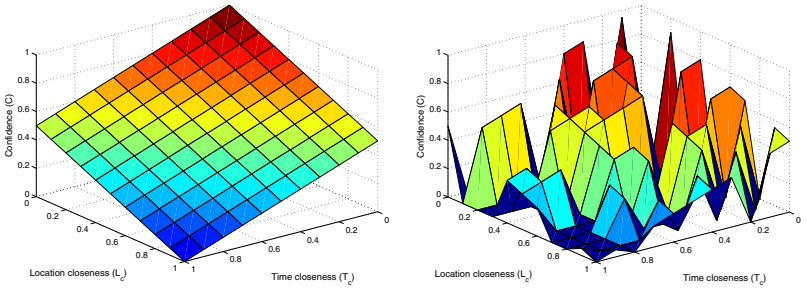
function $L_v(\theta, d_{max}, x_s, y_s, x_c, y_c)$
  Let A is a potential region.
  Let (x_l, y_l) are the lower coordinates of A.
  Let (x_u, y_u) are the upper coordinates of A.
  if $\theta < 90^\circ$ **then**
    $x_u = x_c + d_{max} \cdot \cos\theta$
    $y_u = y_c + d_{max} \cdot \sin\theta$
    $x_l = x_c$
    $y_l = y_c$
  else if $\theta > 90^\circ$ & $\theta < 180^\circ$ **then**
    $x_u = x_c$
    $y_u = y_c + d_{max} \cdot \sin\theta$
    $x_l = x_c + d_{max} \cdot \cos\theta$
    $y_l = y_c$
  else if $\theta > 180^\circ$ & $\theta < 270^\circ$ **then**
    $x_u = x_c$
    $y_u = y_c$
    $x_l = x_c + d_{max} \cdot \cos\theta$
    $y_l = y_c + d_{max} \cdot \sin\theta$
  else
    $x_u = x_c + d_{max} \cdot \cos\theta$
    $y_u = y_c$
    $x_l = x_c$
    $y_l = y_c + d_{max} \cdot \sin\theta$
  end if
  if $(x_l \leq x_s \leq x_u)$ and $(y_l \leq y_s \leq y_u)$ **then**
    return 1; ▷ Sender has provided true location
  else
    return 0; ▷ Sender has provided fake location
  end if
end function

Once all three factors (time closeness, location closeness and location verification) are determined, we calculate the confidence (C) value on a message x_k as follows:

$$C_{x_k} = \left(1 - \frac{L_c + T_c}{2}\right) \times L_v \tag{3}$$

This equation is developed to satisfy the following intuitively described requirements:

- Property 1: If the location closeness factor increases, then the confidence value decreases.
- Property 2: If the time closeness factor increases, then the confidence value decreases.
- Property 3: If the location verification check is fail, then the confidence level should be zero.



(a) $L_v = 1$ (b) L_v is randomly selected (0 or 1), with equal probability

Fig. 5. Confidence measurement analysis

The graphs shown in Figure 5 are obtained by implementing the Equation 3. These graphs illustrates that the required properties are retained in the Equation 3. The left side of the Figure 5(a) shows that; with the increase in location closeness factor the confidence value decreases. This satisfies property 1. The right side of the Figure 5(a) shows that; with the increase in time closeness factor the confidence value decreases. This satisfies property 2. The Figure 5(b) shows (e.g. the index (1,0.8)) that whenever the location verification method L_{verif} returns zero, the confidence value also becomes zero. This satisfies property 3.

3.2 Trust Measurement

Let X be the set of m unique messages (related to the same event) received from n nodes.

$$X = \{x_1, x_2, \ldots, x_m\} \tag{4}$$

For each unique message x_k, we calculate the trust value in the following manner:

$$t_{x_k} = \frac{|x_k|}{n} \times \sum_{i=1}^{|x_k|} C_i \tag{5}$$

where t_{x_k} represents the trust value on message x_k, $|x_k|$ represents the total number of sender nodes who send the message x_k, and $\sum_{i=1}^{|x_k|} C_i$ represents the cumulative confidence value of all the nodes that send message x_k.

Proposition 1: The range of trust value is always between $\left[0, \frac{|x_k|^2}{n}\right]$.

Proof: Let us assume the worst scenario, in which the confidence C evaluation for each peer is zero. Substituting value of C with zero in equation 5 gives the minimum trust value as shown below.

$$t_{x_k} = \frac{|x_i|}{n} \sum_{i=1}^{|x_k|} C_i = \frac{|x_k|}{n} \sum_{i=1}^{|x_i|} 0 = 0$$

Now let us assume the best scenario, in which the confidence C evaluation for each peer is one. If we substitute C with 1 in equation 5, we get the following result.

$$t_{x_k} = \frac{|x_k|}{n} \sum_{i=1}^{|x_k|} C_i = \frac{|x_k|}{n} \sum_{i=1}^{|x_k|} 1 = \frac{|x_k|^2}{n}$$

This gives us the maximum trust value. □

3.3 Decision Logic

At the end of phase 2, we get m trust values as shown below.

$$T = [t_{x_1}, t_{x_2}, \ldots, t_{x_m}] \tag{6}$$

where each trust value corresponds to each unique message related to specific event.

After that, method will take the decision D based on the following logic.

$$D = \textbf{accept}(x_i \in X) | \forall j \;\; t_{x_i} > t_{x_j}, i \neq j \tag{7}$$

It states that accept message x_i that belongs to set X, such that for all values of j, the trust value of the message x_i must be greater than the trust values of the message x_j.

4 Analysis and Evaluation

4.1 Security Resilience Analysis

Definition 1: A message x_k is considered to be *untrustworthy* if:

1. $L_c = 1$ and $T_c = 1$, or
2. $L_v = 0$, or
3. 1 and 2 both.

Definition 2: A node is called *malicious* if it sends *untrustworthy* messages.

Proposition 2: The confidence value of a malicious node is 0.

Proof: From Equation 3, confidence value on message x_k is calculated as:

$$C_{x_k} = \left(1 - \frac{L_c + T_c}{2}\right) \times L_v$$

If x_k is untrustworthy message, then according to the Definition 1, L_c and T_c should be equal to 1. Substituting values of L_c and T_c with 1 in the above mentioned equation gives us the following result.

$$C_{x_k} = \left(1 - \frac{1+1}{2}\right) \times L_v = 0$$

□

Claim 1: Our proposed trust management scheme will not allow malicious nodes to increase the trust value of untrustworthy message.

Proof: Let us assume that, for an event e, node has received two types of messages (x_1 and x_2) from n different nodes. Assume that the message x_1 is received from non-malicious nodes and the message x_2 is received from malicious nodes. Malicious nodes will achieve their objective if:

$$t_{x_2} > t_{x_1}$$

This can also be written as:

$$\frac{|x_2|}{n} \times \sum_{i=1}^{|x_2|} C_i > \frac{|x_1|}{n} \times \sum_{i=1}^{|x_1|} C_i$$

Since, x_2 is received from a malicious node. So, according to the Proposition 2, the confidence value of a malicious node should be 0. Therefore, above inequality will transform into the following:

$$|x_2| \times \sum_{i=1}^{|x_2|} 0 > |x_1| \times \sum_{i=1}^{|x_1|} C_i$$

$$0 > |x_1| \times \sum_{i=1}^{|x_1|} C_i$$

However, this is a contradiction. Hence, it prove that the malicious nodes will not be able to increase the trust value of any untrustworthy message. □

Let M_{x_k} denotes the total number of malicious nodes which send the message x_k. As stated before, let $|x_k|$ represents the total number of sender nodes which send the message x_k. So, $M_{x_k} \leq |x_k|$, and $M_{x_k} > 0$.

Proposition 3: In the presence of malicious nodes, the maximum trust value, the method can assign to the message x_k is $\frac{(|x_k| - M_{x_k})^2}{n}$.

Proof: From Equation 5, we have

$$t_{x_k} = \frac{|x_k|}{n} \times \sum_{i=1}^{|x_k|} C_i$$

If M malicious nodes send message x_k, then the above mentioned equation will transform in the following:

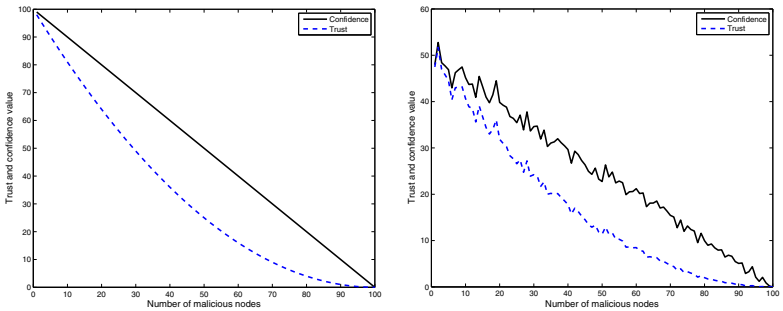
$$t_{x_k} = \frac{|x_k| - M_{x_k}}{n} \times \sum_{i=1}^{|x_k| - M_{x_k}} C_i \tag{8}$$

In this scenario, let us assume the best case, in which the confidence value of all non-malicious nodes is 1. So, $\sum_{i=1}^{|x_k|-M_{x_k}} C_i = |x_k| - M_{x_k}$. Substituting this value in the above-mentioned equation gives the following result.

$$t_{x_k} = \frac{|x_k| - M_{x_k}}{n} \times (|x_k| - M_{x_k}) = \frac{(|x_k| - M_{x_k})^2}{n}. \tag{9}$$

□

Figure 6 shows the behavior of the Equation 8 in two scenarios. In the first scenario, values of the L_c and T_c are set to 0, which means that the confidence value of all non-malicious nodes is 1. In the second scenario, values of the L_c and T_c are randomly selected between 0 and 1. Both graphs show that the trust value decreases with the increase in number of malicious nodes in the network.



(a) $L_c = T_c = 0$ (b) For each message, values of L_c & T_c are randomly selected b/w 0 & 1

Fig. 6. Effect of malicious nodes on trust & confidence values: $N = 100$, $L_v = 1$

Let $t^m_{x_k}$ represents the trust value for a message x_k that is obtained in the presence of malicious nodes.

Claim 2: For message x_k, $t_{x_k} > t^m_{x_k}$.

Proof: Let us prove this claim by contradiction. Assume that

$$t_{x_k} < t^m_{x_k}.$$

From proposition 1, the maximum trust value t_{x_k}, a message x_k can get is $\frac{|x_k|^2}{n}$. From proposition 3, the maximum trust value $t^m_{x_k}$, a message x_k can get is $\frac{(|x_k| - M_{x_k})^2}{n}$. Substituting both values in the above-mentioned inequality gives the following result.

$$\frac{|x_k|^2}{n} < \frac{(|x_k| - M_{x_k})^2}{n}$$
$$= |x_k|^2 < (|x_k| - M_{x_k})^2$$
$$= |x_k| < |x_k| - M_{x_k}$$

However, this is a contradiction, since, $|x_k|$ could not be less than the $|x_k| - M_{x_k}$, because $M_{x_k} > 0$. Thus it proves that, for the message x_k, the trust value obtained in the non-malicious environment will always be greater than the trust value obtained in the malicious environment. □

4.2 Time Complexity Analysis

As stated before, our proposed method works in three phases: 1) Confidence measurement phase, 2) Trust measurement phase, and 3) Decision phase. Let us first derive the time complexity of each phase, and then we will discuss the overall time complexity of the method.

In the confidence measurement phase, for each message, 6 operations (See Eq. 1) are required to calculate location closeness value, 3 operations (See Eq. 2) are required to calculate time closeness value, and k operations are required for location verification. Here, k represents the number of operations that are required to implement Algorithm 1. One can clearly see that the order of complexity of Algorithm 1 is $\mathcal{O}(1)$. After computing L_c, T_c, and L_{verif}, we compute the confidence value on the message x_k. For this, 4 operations are needed (See Eq. 3). So, for a single message, $6 + 3 + k + 4 = k + 13$ operations are required. Let us assume that node has received n messages related to single event e, so the total number of operations required by this phase is: $n(k + 13)$.Note that, here k is constant. So the asymptotic time complexity of this phase is $\mathcal{O}(n)$.

In the trust measurement phase, the number of operations that are required to calculate the trust value of a single message x_k received from $|x_k|$ nodes are: $2 + |x_k|$ (See Eq.5, which has 1 division, 1 multiplication and $|x_k|$ summation). Let us assume that node has received m unique messages from n nodes related to single event e. In that case, total number of operations, which are required to calculate m trust values are:

$$= (2 + |x_1|) + (2 + |x_2|) + \cdots + (2 + |x_m|)$$

Let us assume the worst scenario, in which all n nodes have sent different message. So $n = m$ and $|x_1| = |x_2| = \cdots = |x_m| = 1$. So, total operations that are required to calculate n trust values will be:

$$= (2 + 1) + (2 + 1) + \cdots + (2 + 1) = 3n$$

Hence, the time complexity for the trust measurement phase is also $\mathcal{O}(n)$.

In the decision phase, the proposed method needs to take a decision in favour of the particular message based on the trust values. Let us assume that the

decision module has received n trust values for n unique messages related to a single event e. In order to decide, the proposed method will first sort n messages according to their corresponding trust values (from highest to lowest), and then accept the message x_k, which has the highest trust value. So, number of operations mainly depends on a sorting algorithm. There exist many sorting algorithms that run in linear time, e.g., Counting sort, Radix sort, and Bucket sort [18].

Note that the time complexity of all three modules is linear. Therefore, we can confidently say that our proposed method can compute trust and take decisions in real time.

5 Conclusion and Future Work

Due to high mobility and ephemeral nature of the vehicular networks, establishing and managing trust is a challenging task. Furthermore, if we want to ensure privacy of the user, then things become more complex. Existing trust management schemes that are proposed for the vehicular networks do not efficiently deal with the above-mentioned challenges. Therefore, we have proposed a new trust management scheme that overcomes these limitations. Our proposed method is completely decentralized that makes it easy to implement in the VANETs. Moreover, it is resilient against security attacks on the trust model itself. Furthermore, it has linear time complexity, which makes it suitable to use in real-time. Another, unique feature of the proposed method is that it operates in identity anonymous environment, which ensures user privacy.

The network topology and node density changes constantly and rapidly in the vehicular networks. So, what is its impact on the trust management? By performing simulation-based analysis and evaluation, we can find the answer of this question. This will be left to future research.

References

1. Jiang, D., Delgrossi, L.: IEEE 802.11p: Towards an international standard for wireless access in vehicular environments. In: Proc. of IEEE Vehicular Technology Conference, Singapore, pp. 2036–2040 (2008)
2. ETSI: European Telecommunications Standards Institute. News Release (September 2008), http://www.etsi.org/WebSite/NewsandEvents/2008_09_Harmonizedstandards_ITS.aspx (retrieved: June 12, 2012)
3. Schoch, E., Kargl, F., Weber, M., Leinmüller, T.: Communication patterns in vanets. IEEE Communications Magazine 46, 119–125 (2008)
4. Altan, O.D., Colgin, R.C.: Threat assessment algorithm for forward collision warning (2004)
5. Maïsseu, B.: IVHW:an inter-vehicle hazard warning system. In: Proc. of the International Workshop on Vehicle Safety Communications, Tokyo, Japan (2003)
6. Nadeem, T., Dashtinezhad, S., Liao, C., Iftode, L.: Trafficview: traffic data dissemination using car-to-car communication. ACM SIGMOBILE Mobile Computing and Communications Review 8, 6–19 (2004)

7. Zhang, J.: A survey on trust management for vanets. In: Proc. of the 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA), Biopolis, Singapore, pp. 105–112 (2011)
8. Chen, C., Zhang, J., Cohen, R., Ho, P.H.: A trust modeling framework for message propagation and evaluation in vanets. In: Proc. of the 2nd International Conference on Information Technology Convergence and Services (ITCS), Cebu, Philippines, pp. 1–8 (2010)
9. Nekovee, M.: Vehicular communications and networks (June 4, 2010), http://www.radio.feec.vutbr.cz/kosy/soubory/maziar/Nekovee_lecture_2_fulltext.pdf (retrieved: May 12, 2012)
10. Shaikh, R.A., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., Song, Y.-J.: Group-based trust management scheme for clustered wireless sensor networks. IEEE Transaction on Parallel and Distributed Systems 20, 1698–1712 (2009)
11. Raya, M., Papadimitratos, P., Gligor, V., Hubaux, J.: On data-centric trust establishment in ephemeral ad hoc networks. In: Proc. of the 27th Conference on Computer Communications (INFOCOM 2008), Phoenix, USA, pp. 1238–1246 (2008)
12. Huang, D., Hong, X., Gerla, M.: Situation-aware trust architecture for vehicular networks. IEEE Communications Magazine 48, 128–135 (2010)
13. Minhas, U.F., Zhang, J., Tran, T., Cohen, R.: Towards expanded trust management for agents in vehicular ad-hoc networks. International Journal of Computational Intelligence: Theory and Practice (IJCITP) 5, 3–15 (2010)
14. Patwardhan, A., Joshi, A., Finin, T., Yesha, Y.: A data intensive reputation management scheme for vehicular ad hoc networks. In: Proc. of the 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, California, USA, pp. 1–8 (2006)
15. Gómez Mármol, F., Martínez Pérez, G.: Trip, a trust and reputation infrastructure-based proposal for vehicular ad-hoc networks. Journal of Network and Computer Applications 35, 934–941 (2012)
16. Huang, Z., Ruj, S., Cavenaghi, M., Nayak, A.: Limitations of trust management schemes in vanet and countermeasures. In: Proc. of the IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Toronto, ON, Canada, pp. 1228–1232 (2011)
17. Gerlach, M., Guttler, F.: Privacy in vanets using changing pseudonyms-ideal and real. In: Proc. of the IEEE 65th Vehicular Technology Conference (VTC 2007 Spring), Dublin, Ireland, pp. 2521–2525 (2007)
18. Pandey, H.: Design Analysis and Algorithms. Laxmi Publications Pvt. Ltd. (2008)