IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

Multi-hop interpersonal trust assessment in vehicular *ad-hoc* networks using three-valued subjective logic

ISSN 1751-8709
Received on 2nd July 2018
Revised 26th October 2018
Accepted on 5th November 2018
E-First on 18th February 2019
doi: 10.1049/iet-ifs.2018.5336
www.ietdl.org

Muhammad Sohail[1], Liangmin Wang[1] ✉, Shunrong Jiang[1], Samar Zaineldeen[1], Rana Umair Ashraf[1]

[1]*School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, Jiangsu, People's Republic of China*

✉ *E-mail: wanglm@ujs.edu.cn*

Abstract: Future vehicular networks need multi-hop trusted information among car manoeuvres as a solution to the persistent problem of road safety, and news sharing. However, malicious users in vehicular networks can also disseminate fake information among each other. Traditional public key infrastructure is not an efficient solution for recognising these malicious users, as they all have authorised entities. To cope with this problem, this study highlights novel idea, i.e. three-valued subjective logic (3VSL) as a trust model for multi-hop trust assessment among users in vehicular *ad-hoc* network (VANET). Trust among vehicle users is represented in the form of opinion derived from 3VSL and updated frequently due to vehicles random movement on the road. To support the authors' proposed scheme, this study contains two parts in simulation, i.e. numerical and experimental analyses. Numerical analysis shows that 3VSL gives accurate trust assessment even with a bridge or random network topology, which is ignored previously by edge splitting. In the experimental part, we extend widely accepted *ad-hoc* on-demand distance vector routing protocol by directly applying trust fields to the routing table. The simulation experiment shows that their scheme achieves better performance in term of throughput and latencies in low mobility VANET scenario.

1 Introduction

The growing need for intelligent transportation system, road safety and Internet services had led the interest of industry and research academia to integrate modern wireless services into the vehicular *ad-hoc* network (VANET). These vehicular networks impose new security challenges due to its high speed and dynamics [1, 2]. Therefore, we need a novel guaranteed security solution for the VANET before it is deployed. In future intelligent transportation, many car manoeuvres will rely on shared information among neighbour vehicles, so the credibility of disseminated information is a key priority. Recently trust management emerged as the promising candidate to provide lightweight security solutions in *ad-hoc* networks [3, 4]. The idea of trust comes from social science, which defines trust as a degree of subjective opinion about the behaviour of an entity in a particular context [5].

Moreover, despite much-proposed security solutions to VANET, e.g. cryptographic algorithms, public key infrastructure (PKI), and privacy-preserving schemes there is a lack of trust and uncertainty management [6]. Though PKI act as a baseline of initial defence with the help of central services, further, it helps in the identification of concerned vehicle but not about tried-and-true. [7]. The PKI or signature-based security solutions also need cloud-assisted services for storing these public and private keys [8]. However, malicious vehicles can broadcast false information and traditional PKI cannot recognise these malicious users because they all have authorised entities. In this situation, we need a trust management system that works purely in a distributed manner, so vehicles can authenticate and tackle time critical messages itself, like highway merging. Also, other disseminated information among vehicle users like road construction/congestion must be genuine and trustworthy to save the time. Referring to Fig. 1*a*, the vehicle onboard sensors detect that there is road construction ahead, so it informs the roadside unit (RSU) and neighbour vehicles as well to get diverged. In Fig. 1*b*, there is conflicting news about road construction, some of the malicious vehicles spread the fake news to get road clear. If the trustworthy of the sensed data assessed incorrectly, then there might be a chance of traffic jam or even worse, i.e. road accidents, because in this scenario many vehicles will be remapped to the same route if the false disseminated alarms remain undetected and thus harmful to ongoing VANET, as shown in Fig. 1*c*.

Further, vehicles on the road not necessarily move regularly, the topology can be random. How to cope with this dynamic vehicular topology and to assess accurate data based on the trust score between itself and information provider in multi-hop vehicles communication, three-valued subjective logic (3VSL) answers [9]. Therefore, in numerical analysis, our proposed trust model proved to be correct by applying the assess trust algorithm in arbitrary

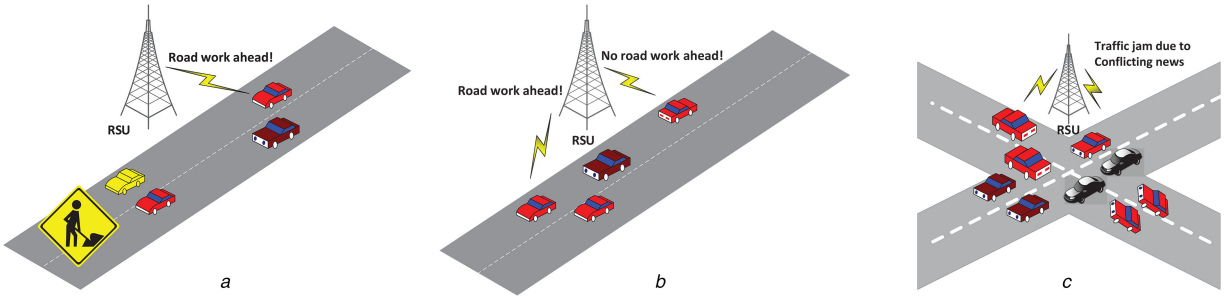


Fig. 1 *Traffic monitoring results in VANET*

(a) Result of trusted vehicle information, so vehicles may use divergence to save time, ***(b)*** Result of conflicting information, a malicious vehicle can spread false news to get road clear, ***(c)*** Result of having conflicting news about road clearance both at the same time

Table 1 List of symbols

Symbol	Description
VANET	vehicular *ad-hoc* network
3VSL	three-valued subjective logic
AODV	*ad-hoc* on-demand distance vector
RSU	road side unit
PKI	public key infrastructure
V2R, V2I, V2V	vehicle to (RSU, infrastructure, vehicle)
AVT	arbitrary vehicular topology
w_B^A	trust opinion of vehicle A about B
$A\Theta B$	consensus operation between vehicles A and B
$A\Delta B$	discount operation between vehicles A and B
$\Delta(w_{AB}, w_{BC})$	trust of vehicle A in C based on B's advise
$\Theta(w_{AC}, w_{BC})$	trust of vehicles A and B in C

vehicular network topology, which is previously ignored by edge splitting using subjective logic [10]. Therefore, the problem is how to solve the trustworthiness from truster to trustee in arbitrary network topology is explained using the graph theory example. Given an arbitrary vehicular topology (AVT) such that $G(V_S, V_T), \forall s$ and t such that $e(s,t) \notin E$ and $\exists$ at least one path from s to t, how will a stranger vehicle user s rely on t, after its trust assessment based on its existing direct and recommended connections in AVT? Also, in the experimental part, we validate the accuracy of extended *ad-hoc* on-demand distance vector (AODV) routing protocol using 3VSL. The interested users may refer to [11] for understanding the enhanced AODV using subjective logic. Following are the contributions of this paper.

i. First, our proposed scheme took advantage of a novel 3VSL trust model and enhanced AODV routing protocol to solve multi-hop trust assessment in an arbitrary vehicular network topology. 3VSL implements discounting and combining operations recursively on subtrees to reach the upper level from information receiver to sender, second trust information is directly added with the extended AODV in route request, route reply, and route warning. These two amendments help to reduce extra routing overhead by directly exchanging trust information in the route packets, which update the trust in the corresponding peer accordingly.
ii. Second, numerical analysis and experimental setup are conducted. Impact of bridge network topology is analysed in a numerical study, and results indicate that edge splitting ignores much evidence in final computation. In the experimental part, we extend widely accepted reactive routing protocol, i.e. AODV using 3VSL. Performance analysis among trust model enabled AODV (proposed scheme), authenticated anonymous secure routing (AASR) [12] and original AODV is conducted. Our proposed scheme proved to be accurate for better performance under different mobility settings and an increasing number of malicious vehicles.
iii. Third, our proposed scheme can be implemented using advanced routing protocols for peer-to-peer user trust assessment. Also, it can be used in online social networks for multi-hop interpersonal trust assessment [11, 13].

2 Background

2.1 Related work

Trust models can be classified into two categories, i.e. central and distributed. In a central system, the vehicle user relies more on a trusted third party, which is a bottleneck for the whole system. Extensive research has been done to support VANET infrastructure using cloud services [14, 15]. In a distributed system, vehicles can make a small social network within the transmission range without the central agent and may enjoy different services [13], but its decentralised nature needs significant research to address potential security issues. Therefore, industry and academia showed their interest in trust model based security solutions for VANET [16, 17]. In our proposed scheme one possibility is to build and maintain the opinion table on each vehicle in a distributed manner by the car manufacturing industry. Using this opinion table a vehicle can quickly determine whether the information provided is trustful enough to believe it or not. Although without central agent and computation servers the system's real-time performance will be significantly degraded, as the CA has large storage, computation power with complete security infrastructure.

In addition, vehicle users before joining the network are suspicious about network behaviour and other vehicles as well. To deal with this uncertainty Josang in [18] proposed the subjective logic framework. The authors in [19–21], also proposed a trust model based routing between unknown users in mobile *ad-hoc* network using subjective logic. Ren *et al.* in [22], also made use of subjective logic based consensus techniques to mitigate trust fluctuations caused by environmental factors. Rens *et al.* also used the subjective logic framework for misbehaviour detection in V2V networks [23, 24]. However, in light of works mentioned above, one major drawback of subjective logic is only to consider prior uncertainty, which leads to false computation in the final opinion. To cope with this problem, we rely on novel 3VSL trust model to nicely deal prior and posterior uncertainty both at the same time.

Moreover, In recent years many complex cryptographic schemes [25, 26] along with anonymous security solutions such as trapdoor, onion routing, and group-based signature [27], AASR [12] were proposed to detect misbehaviour activity by adversary, these solutions have lack of trust management, ignore uncertainty in a distributed environment and heavily rely on cryptographic operations. Therefore, these are not an efficient solution for the said environment. *Ad-hoc* networks, especially like VANET, needs an uncertainty/trust management solutions so that vehicles can authenticate each other in a distributed manner. In light of the proposed schemes, we argue that our solutions can provide promising results using a simplified trust model, i.e. 3VSL, which will be explained in Section 3. Also, a list of acronyms is given in Table 1 for ease of readers.

2.2 Dirichlet distribution

It is important here to introduce the Dirichlet distribution that we have used in trust modelling. The Dirichlet distribution gives a solid mathematical foundation for measuring uncertain values using historical data or feedback. Although, Beta distribution [28] is well known to deal with binary evidence space α, β, but in case of multiple evidence space (α, β, γ) Dirichlet distribution is the right choice [29].

Dirichlet distribution is a sequence of observations having k possible outcomes with k positive real parameters $\alpha(x_i), i = 1, \ldots, k$, in the form of compact vector notation $\boldsymbol{p} = p(x_i | 1 \le i \le k)$ denotes the k-component random probability variable and a vector $\boldsymbol{\alpha} = (\alpha_i | 1 \le i \le k)$ denotes the random observation variable of k components such that $[\alpha(x_i)]_i^k$. The general form of the Dirichlet distribution is as

$$f(\boldsymbol{p}|\boldsymbol{\alpha}) = \frac{\Gamma\left(\sum_{i=1}^{k} \alpha(x_i)\right)}{\prod_{i=1}^{k} \Gamma\alpha(x_i)} \prod_{i=1}^{k} p(x_i)^{\alpha(x_i)-1} \quad (1)$$

The 3VSL evidence space using Dirichlet distribution can be modelled as follows:

$$f(P_{b|\alpha}, P_{d|\beta}, P_{n|\gamma}) = \frac{\Gamma(\alpha+\beta+\gamma)}{\Gamma_{(\alpha)} + \Gamma_{(\beta)} + \Gamma_{(\gamma)})} \cdot P_b^{\alpha-1} \cdot P_d^{\beta-1} \cdot P_n^{\gamma-1} \quad (2)$$

Here (α, β, γ) control the shape of the distribution, where P_b, P_d and P_n show the probabilities of the three states. In the absence of any solid evidence, the prior evidence for each event is considered to be one, i.e. $(\alpha = 1, \beta = 1, \gamma = 1)$. Based on this assumption the prior probability of each event will be 1/3, and its reasonable as the minimum probability in the Dirichlet distribution and it is observed as prior uncertainty of each event. The 3VSL opinion space is

mapped against positive p, negative n, and neutral o captured evidence as follows:

$$b_j^i = \frac{p}{p+n+o+3}, \quad d_j^i = \frac{n}{p+n+o+3}$$
$$n_j^i = \frac{o}{p+n+o+3}, \quad e_j^i = \frac{3}{p+n+o+3} \tag{3}$$

3 Subjective logic fundamentals

Subjective logic is a kind of probabilistic reasoning, first proposed by Josang and Bhuiyan [10], to manage uncertainty between unknown users in a particular context such as trust about driving a car. Subjective logic uses the form of opinion metric to express the degree of ignorance in a particular context. The opinion metric in subjective logic is modelled using binary state space with Beta distribution. Therefore, in the absence of any observed evidence, the prior probability of each event will be 1/2.

Opinion space using subjective logic can be expressed as $\omega = (b, d, u, a)$. Here b, d, u show believe, disbelief and uncertainty, respectively. The total probability of evidence space will be $b + d + u = 1$. The base rate $a \in [0, 1]$ is used to compute an opinion's probability expectation value before the operation, which can be written as $E(\omega_x^A) = b + au$. Further, we also have consensus and discounting operations in subjective logic but these are limited to prior uncertain value. Due to the page limit, we did not mention the equations here, an interested user may refer to [10, 18].

3.1 Three-valued subjective logic

Monitoring user behaviour in VANET based on prior communication pattern and random topologies involves considerable uncertainty. To deal with this uncertainty, we adopt 3VSL framework as our trust model [9]. The following are the major definitions in 3VSL.

3.1.1 Trust representation: An opinion space in 3VSL contains multinomial evidences (trust, distrust, prior and posterior uncertainty). Prior uncertainty that is produced due to the lack of evidence, while posterior uncertainty produces during trust propagation in the case of evidence distortion

$$\omega_B^A = \left(b_B^A, d_B^A, n_B^A, e_B^A\right) \rightarrow \left(b_j^i, d_j^i, n_j^i, e_j^i\right), \quad i \rightarrow j$$

The component in 3VSL opinion space includes b_B^A, d_B^A, n_B^A and e_B^A showing the probability of trust, distrust, posterior and prior uncertainty. The posterior uncertainty n_B^A is generated due to evidence distortion between two users. The prior uncertainty e_B^A will be a maximum in the case of two vehicle users have never interacted before or just joining the existing VANET, i.e. maximum uncertainty. Based on this, new evidence space 3VSL distinguishes the posterior and prior uncertainty exists in the trust, the original and distorted opinion, and redesign the combining and discounting operations.

3.1.2 Direct trust assessment: We define vehicle i's direct opinion (${}^iw_j^{\text{dir}}$) towards vehicle j depending on the collected evidence from one-to-one interaction with j. This evidence is collected by forwarding related information to a vehicle j and then monitoring the successive forwarding of the same packet. If the information is forward completely as it is, then this behaviour is considered as benign. Alternatively, if the information is forged/ dropped then this act is considered as malicious behaviour. After noticing this malicious act vehicle i will exclude vehicle j for further correspondence, until the completion of flow due to its malicious behaviour.

Soon after the recent interaction vehicle, i revises its opinion about vehicle j as positive (p) or negative (n) evidence. Also, neutral evidence (o) is revised as the time of no interactions between vehicles i and j. After that vehicle i updates its direct opinion towards vehicle j based on the captured positive, negative and neutral evidences as (${}^iw_j^{\text{dir}}$). The evidence to opinion mapping can be calculated using (3), that defined in Section 2.2.

3.1.3 Indirect trust assessment: Based on our proposed scheme, a vehicle gathered direct and indirect observation about its neighbour vehicles and combined them using discounting and consensus operations defined in 3VSL. In this manner, a vehicle can make the relative objective judgment about other vehicle's trustworthiness even in a case; several vehicles are lying.

3.2 Consensus operation in 3VSL

In a parallel topology, opinions should be fused and combined on fair bases, so that resultant opinion reflects all evidences. Here, we introduce consensus operation, which is based on Dirichlet distribution. Symbolically, we can use theta Θ to represent the combining operation. If we have $w_1 = (b_1, d_1, n_1, e_1)$ and $w_2 = (b_2, d_2, n_2, e_2)$ then $\Theta = (w_1, w_2)$ is called combining operation between two parallel paths. Each component in opinion space can be obtained using the following equation:

$$b_{12} = \frac{e_2 b_1 + e_1 b_2}{e_1 + e_2 - e_1 e_2}, \quad d_{12} = \frac{e_2 d_1 + e_1 d_2}{e_1 + e_2 - e_1 e_2}$$
$$n_{12} = \frac{e_2 n_1 + e_1 n_2}{e_1 + e_2 - e_1 e_2}, \quad e_{12} = \frac{e_1 e_2}{e_1 + e_2 - e_1 e_2} \tag{4}$$

It can be easily proved that combining operation is commutative and associative

$$\Theta(w_1, w_2) \equiv \Theta(w_2, w_1) \text{ and } \Theta(w_1, \Theta(w_2, w_3) \equiv \Theta(\Theta(w_1, w_2), w_3) \tag{5}$$

for multiple parallel opinions between n users, the final opinion can be written as follows:

$$\Theta(\Theta(\Theta(w_1, w_2), \ldots), w_n) \simeq \Theta(w_1, w_2, \ldots, w_n)$$

3.3 Discounting operation in 3VSL

Let A, B and C be three vehicles and $\omega_B^A = (b_1, d_1, n_1, e_1)$ shows vehicle A opinion about B's trustworthiness and $\omega_C^B = (b_2, d_2, n_2, e_2)$ shows vehicle B opinion about C's trustworthiness. The final opinion $\omega_C^{A.B}$ shows A opinion about C using B's recommendation. Symbolically we can use triangle Δ to represent this operation

$$\Delta(\omega_B^A, \omega_C^B) = \begin{cases} b_{12} = b_1 b_2, & d_{12} = b_1 d_2 \\ n_{12} = 1 - b_1 - d_2 - e_2, & e_{12} = e_2 \end{cases} \tag{6}$$

where $\Delta(\omega_B^A, \omega_C^B)$ shows A's opinion on C using B's advice to A. User A can discount multiple agents to gain its trust on vehicle C. During this process some evidences from ω_B^A are distorted because A has changing trust opinion about B time being. The distorted evidences from ω_B^A will be saved into a neutral state of the final opinion, i.e. ω_C^A, while prior uncertainty remains same, as shown in Fig. 2. Evidence distorted comes from belief and disbelief of opinion ω_B^A and are saved into the posterior uncertainty space of ω_C^A, so ω_C^B and ω_C^A will have the same amount of evidences in the resultant opinion.

3.4 Difference between distorting and original opinion

Referring to a discounting operation in 3VSL as depicted in Fig. 2, we have direct opinions w_B^A and w_C^B. Here, w_C^A is distorted opinion between vehicles A and C and comes after discounting of vehicle B as $w_C^A = \Delta(\omega_B^A, \omega_C^B)$. Meanwhile, some evidence from w_B^A are distorted as a result of discounting operation and transferred to the posterior state of w_C^A. The evidence space of opinion $w_C^A = \Delta(\omega_B^A, \omega_C^B)$ remains same as of w_C^B's, because discounting operation is associative but not commutative

$$\Delta(w_1, w_2) \neq \Delta(w_2, w_1)$$

$$\Delta(\Delta(w_1, w_2), w_3) \equiv \Delta(w_1, \Delta(w_2, w_3)$$

$$\Delta(\Delta(\Delta(w_1, w_2), \ldots), w_n) \simeq \Delta(w_1, w_2, \ldots, w_n)$$

Here, prior uncertainty is kept unchanged and posterior uncertainty to store distorted evidence during trust propagation. Now consider the following lemma.

Lemma 1: Let w_1, w_2 and w_3 are three opinions, then

$$\Delta(w_1, \Theta(w_2, w_3)) \equiv \Theta(\Delta(w_1, w_2), \Delta(w_1, w_3)) .$$

However,

$$\Delta(\Theta(w_1, w_2), w_3) \neq \Theta(\Delta(w_1, w_3), \Delta(w_2, w_3))$$

.

We omit the details here as they can be proved easily. From the above equations, we concluded that in a 'final trust computation, discounting opinions (recommendations) can be used no of times, as compared to original (direct) opinion'.

4 Arbitrary vehicular topology

VANET is unique due to its speed and infrastructure, thus may have random topologies time being. Series and parallel topologies can be solved by both subjective logic and 3VSL, but the bridge and arbitrary topologies can be accurately computed by 3VSL. Starting from vehicles C to A in a backward direction, bridge topology can be expressed as a binary decomposition tree as shown in Fig. 3*b*. Here AB is used twice being distorted evidence, which is permitted by Lemma 1. Another example is depicted in Fig. 3*c*, entities are connected irregularly from V_S to V_T. We can explain this by using the graph theory example in Theorem 1. Based on Theorem 1, we proposed a trust assessment algorithm to apply in an AVT, where G shows an original graph, V_S and V_T denote the truster and trustee, respectively.

Theorem 1: Given an arbitrary two-terminal directed graph $G(V, E)$, where V_S, V_T are two terminals. Edge $e(u, v)$ represents the opinion w_v^u between V_S and V_T. Applying to discount and combining operation, the overall opinion $w_{V_T}^{V_S}$ is solvable and has a unique solution.

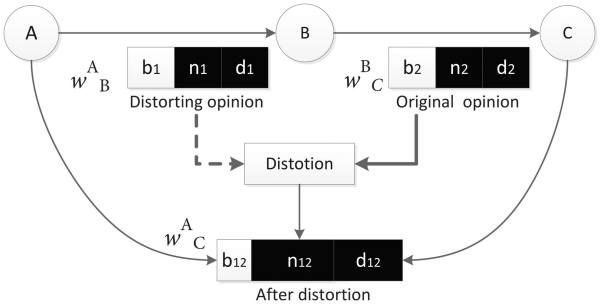


Fig. 2 *Effect of the discounting operation in 3VSL. The opinion w_C^A is a distorted opinion as comes after discounting vehicle B*

Proof: We prove the solution recursively, i.e. reducing the original problem into subproblems and continue reducing subproblems until the base case is solved and has a unique solution.

As from Fig. 3*c*, let m nodes connecting to V_T as $(t_1, t_2, \ldots, t_m)$, i.e. $e(t_i, V_T) \in E$ and $i \in [1, m]$. Also, let n vehicles $(s_1, s_2, \ldots, s_n)$ being connected to V_S, i.e. $e(V_S, s_j) \in E$ and $J \in [1, n]$. We have two cases to describe this.

Case 1: if we have only one connected vehicle to V_T such that $m = 1$, then $w_{V_T}^{V_S} = \Delta(w_{t_1}^{V_S}, w_{V_T}^{t_1})$.

Case 2: if we have more than one connected vehicles, i.e. $m > 1$, so using Lemma 1,

$$w_{V_T}^{V_S} = \Theta(\Delta(w_{t_1}^{V_S}, w_{V_T}^{t_1}), \Delta(w_{t_2}^{V_S}, w_{V_T}^{t_2}), \ldots, (\Delta(w_{t_m}^{V_S}, w_{V_T}^{t_m})) \quad (7)$$

It is stated that $w_{V_T}^{V_S}$ is unique and solvable if and only if $w_{t_i}^{V_S}$ is solvable, where $w_{t_i}^{V_S}$ is the result of subproblem with subgraph $G' = G - \sum e(t_i, V_T) - V_T$. For the second case, the topology can be random and yet unknown for sure, it is possible that all t_i are connected at a certain node u.

If $u = V_S$, then $\widehat{V_S u t_i V_T}$ are parallel and can be combined. If $u \neq V_S$, then $w_{V_T}^{V_S}$ can be computed as (1) the consensus of $\widehat{V_S u t_i V_T}$, or (2) consensus of $\widehat{u t_i V_T}$ first and discount it by $w_u^{V_S}$. According to Lemma 1, both yield the same results.

The original topology, G is reduced into G' in the sense that $|E| = |E| - m$ and $|V| = |V| - 1$. Applying reductions on subproblems recursively, finally, the base case such that $|V| = 2$, and $|E| = 1$ will arise and topology from $w_{V_T}^{V_S}$ will be solvable and unique (see Fig. 4). □

5 Numerical analysis

In a mathematical evaluation using discounting and combining operations, we have considered parallel and bridge network topologies and adjust T (trust) and e (prior uncertainty) parameters to see their effect on trust model to verify whether it works fine as said. For simplicity, we have considered total evidence value in opinion as λ, i.e. $\lambda = \alpha + \beta + \gamma$.

5.1 Discounting operation

The word discount used in 3VSL, as A agrees on B's advise to know C's truthfulness, so as opinion w_{AC} is derived from $\Delta(w_{AB}, w_{BC})$. Let, suppose initial evidence in opinion as a total is 20 such that $\lambda_{AB} = \lambda_{BC} = 20$. In this analysis by changing the number of positive evidence, i.e. α_{AB} and α_{BC} from 0 to 20, we investigate the accuracy of 3VSL by observing the expected belief of w_{AC}.

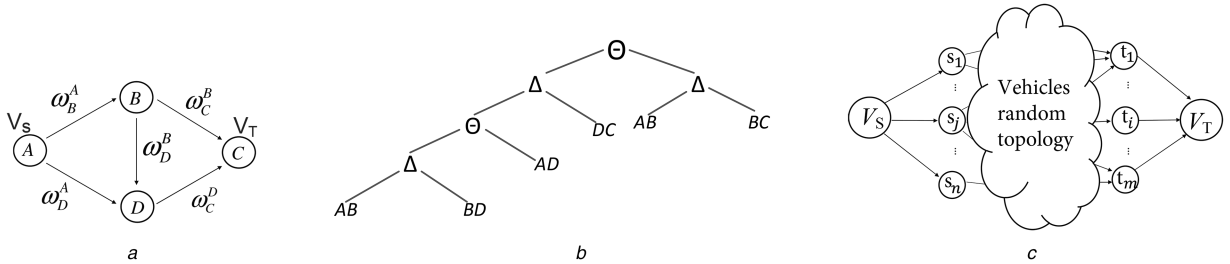


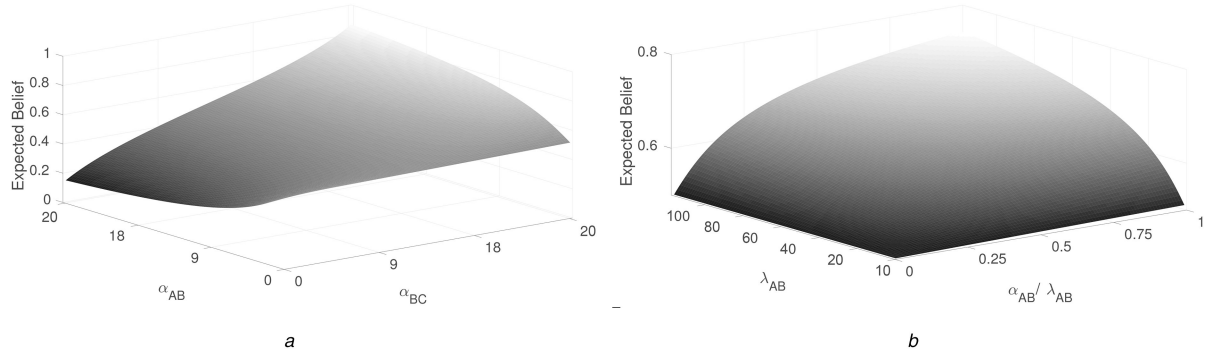
Fig. 3 *Network topologies of connected vehicles in VANET*

(a) Example of bridge network topology having bridge opinion w_D^B, ***(b)*** Binary decomposition tree of bridge topology, it works hop by hop fashion using discounting and consensus operations, ***(c)*** Vehicle users from V_S to V_T are connected in an arbitrary fashion

Require: A directed graph G with V_S (truster) and V_T (trustee) and maximum search depth is h.;
Ensure: V_S's opinion on V_T, $w_{V_T}^{V_S}$

1: $n \leftarrow 0$
2: **if** $h > 0$;
3: **for each** incoming edge $e(t_i, V_T) \in G$ do ;
4: **if** $(t_i = V_S)$;
5: $w_i \leftarrow w_{t_i}^{V_S}$;
6: else;
7: $G' \leftarrow G - e(t_i, V_T)$;
8: $w_{t_i}^{V_S} \leftarrow Trust - Assessment(G', V_S, t_i)$;
9: $w_i \leftarrow \triangle(w_{t_i}^{V_S}, w_{V_T}^{t_i})$;
10: **endif**;
11: **if** $n > 1$;
12: $w_{V_T}^{V_S} = \Theta(w_1 .... w_n)$;
13: $w_{V_T}^{V_S} = w_n$;
14: **end for**;
15: **else**;
16: $w_{V_T}^{V_S} = (0, 0, 0, 1)$;
17: **endif**;

Fig. 4 *Algorithm 1: assess trust* (G, V_S, V_T)



a *b*

Fig. 5 *Numerical Analysis to validate 3VSL's Discounting operation by changing T(trust) and e (Prior uncertainty)*
(a) Effect of high belief on discounting operation, ***(b)*** Effect of uncertainty and belief on discounting operation

It is clear from Fig. 5*a*, when α_{AB} and α_{BC} increases, the expected belief of opinion $E_{w_{AC}}$ is also increasing because both are positive evidences. It means that if the belief of A is high in B, so it will also trust C regarding B's advice and vice versa. When α_{AB} and α_{BC} having low values than expected belief of opinion $E_{w_{AC}}$ tends to approach 0.5, which indicates that A holds a self-opinion on C because A has less trust in B, so discounting B's opinion for C's trustworthiness is useless.

To further understand the impact of the evidence, we have also considered the influence of uncertainty and changed values of α_{AB}/λ_{AB} as from 0 to 1 and λ_{AB} from 0 to 100. In this analysis, we keep the original opinion w_{BC} unchanged such that $w_{BC} = (20, 5, 0)$. As, we can see in Fig. 5*b*, when λ_{AB} has high value, $E_{w_{AC}}$ increases as α_{AB}/λ_{AB} increases. Also, as λ_{AB} value decreases, $E_{w_{AC}}$ tends to close 0.5. This scenario tells that if A has high trust in B, i.e. larger λ_{AB}, she relies more on B's advice to make her opinion on C's trustworthiness.

5.2 Consensus operation

In discounting operation, we elaborate on the impact of belief and uncertainty by changing the values of λ_{AB} and α_{AB} which can also be written using T_B^A and e_B^A such that,

$$(T_B^A \times (1 - e_B^A), (1 - T_B^A) \times (1 - e_B^A), 0, e_B^A) \tag{8}$$

over the continuous range [0, 1]. Let's consider the general parallel topology case is having $w_C^{A_1}$ and $w_C^{A_2}$ as two opinions from A to C. We kept $w_C^{A_2}$ as constant opinion $(0.7, 0.1, 0, 0.2)$ (high trust), while $w_C^{A_1}$ is a random opinion like $(0.125 \times (1 - e_C^{A_1}), 0.875 \times (1 - e_C^{A_1}), 0, e_C^{A_1})$ (high distrust) with variable prior uncertain values. As shown in Fig. 6*a*, when $e_C^{A_1}$ is less than $e_C^{A_2}$, then expected belief using combining operation $E(\Theta(w_C^{A_1}, w_C^{A_2}))$ tends to approach $w_C^{A_1}$. When $e_C^{A_2} < e_C^{A_1}$, then $E(\Theta(w_C^{A_1}, w_C^{A_2}))$ tends to approach $w_C^{A_2}$. Thus combining two opinions yields a more realistic value with less uncertainty and positive evidence.

After that, we evaluated how belief affects the combining operation,

$$w_C^{A_2} = (0.7, 0.1, 0, 0.2) \text{ and } w_C^{A_1} = (0.8 \times T_C^{A_2}, 0.8 \times (1 - T_C^{A_2}), 0, 0.2) \tag{9}$$

with varying beliefs. In Fig. 6*b*, when $T_C^{A_2}$ and $T_C^{A_1}$ are close, then expected belief $E(\Theta(w_C^{A_1}, w_C^{A_2}))$, a little higher then both $w_C^{A_2}$ and $w_C^{A_1}$. Also, when $T_C^{A_1}$ and $T_C^{A_2}$ have different values, then $E(\Theta(w_C^{A_1}, w_C^{A_2}))$ tends to close mean of $E(w_C^{A_1})$ and $E(w_C^{A_2})$. From these analyses, we conclude that combining opinions having same prior uncertainty and belief will enhance the original opinions, due to more evidences. While combining opinions with different beliefs and equal prior uncertain values will neutralise these two opinions.

5.3 Analysis of bridge network topology

A special feature of 3VSL is that it can also handle bridge network topology, as shown in Fig. 3*a*, while conventional subjective logic fails to address this issue because it has to remove certain edges [10].

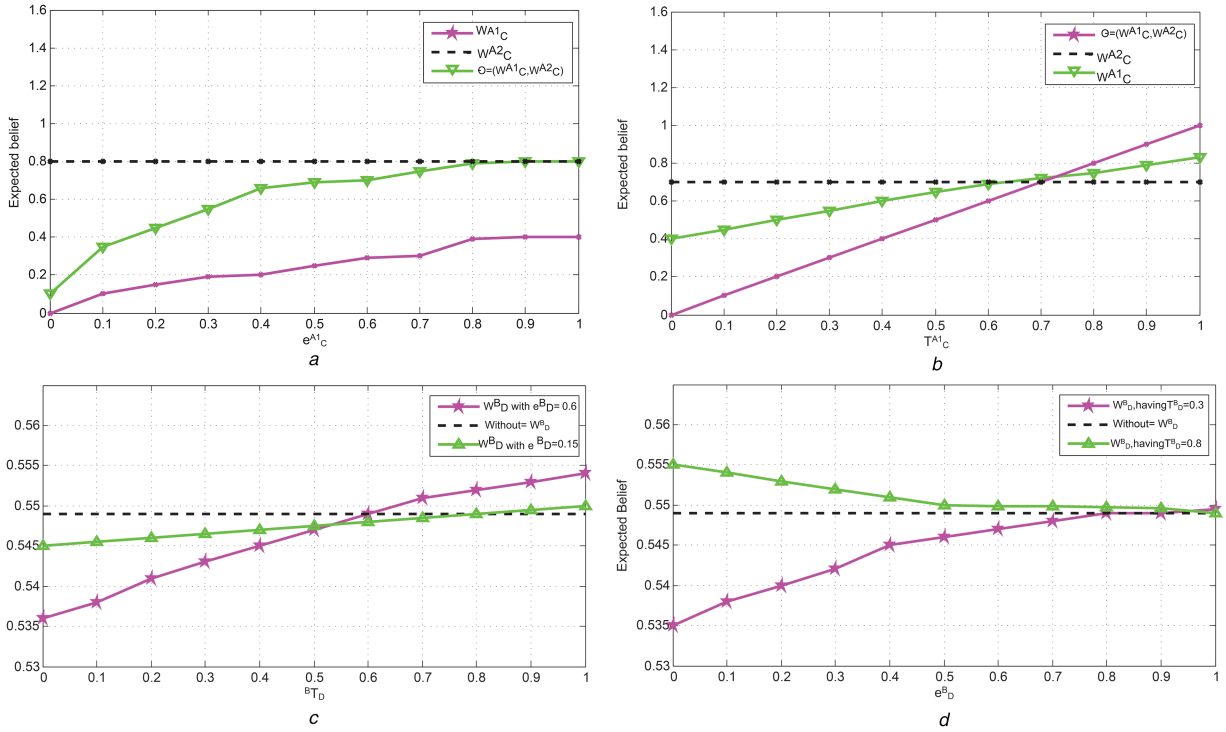


Fig. 6 *Numerical Analysis to validate 3VSL's Consensus operation by changing T(trust) and e (Prior uncertainty) and in solving bridge network topology*
(a) Effect of prior uncertainty on consensus operation, ***(b)*** Effect of trust variation on consensus operation, ***(c)*** Effect of bridge opinion's belief on the resulting expected belief, ***(d)*** Effect of bridge opinion's prior uncertainty on the resulting expected belief

Table 2 Standard and trust model enabled AODV

Standard AODV	Enhanced AODV using 3VSL
destination Ip address	destination Ip address
destination seq number	destination seq number
...	...
hop count	same
...	...
expiry time	expiry time
empty	positive event
empty	negative event
empty	opinion metric
empty	trust update

In subjective logic, bridge opinion is normally ignored by network canonisation and this becomes a two terminal parallel network topology where A link to C using two paths such that $\widehat{ABC}$ and $\widehat{ADC}$. To see the impact of bridge opinion on parallel topology, we set four opinions

$$w_B^A, w_C^B, w_D^A \text{ and } w_C^D \text{ as}$$
$$(0.7, 0.1, 0, 0.2), (0.7, 0.1, 0, 0.2), \quad (10)$$
$$(0.6, 0.2, 0, 0.2), \text{ and } (0.6, 0.2, 0, 0.2)$$

respectively. Then, the effect of bridge opinion w_D^B is validated using $(T_D^B \times (1 - e_D^B), (1 - T_D^B) \times (1 - e_D^B), 0, e_D^B)$.

We have taken high and low prior uncertain values, e.g. $e_D^B = 0.6$ and $e_D^B = 0.15$, and vary trust by changing T_D^B from 0 to 1. It can be seen in Fig. 6*c*, when prior uncertainty is low such that $e_D^B = 0.15$, then expected belief of the bridge topology tends to close T_D^B of the parallel topology. When $e_D^B = 0.6$ it approaches to T_D^B but not as well as with $e_D^B = 0.15$. It is concluded that bridge opinion is a certain one, it impacts on the final result could not be ignored.

Secondly, we vary e_D^B from 0 to 1 and keeping $(T_D^B = 0.7)$ high trust value and $(T_D^B = 0.3)$ as low trust value. It can be seen from Fig. 6*d*, when e_D^B has low value, the impact of bridge topology cannot be omitted. When e_D^B is high, then expected belief gets close to parallel topology. Further, with high e_D^B i.e. (lack of positive evidences), the bridge opinion has not much effect on the final opinion and can be omitted as what subjective logic does. Also, it is noticed that the larger belief of the bridge opinion w_D^B leads to a higher expected belief than the parallel topology and inverse is true also.

6 Experimental analysis

In the experimental part, we have used NS-3.20 [30] platform using an Ubuntu-14.05 operating system for performance evaluation among different routing protocols running on Intel core i5 Lenovo machine. Here, we considered a scenario in which vehicles make small social groups having low mobility. After that, we applied our trust model, i.e. 3VSL combined with AODV routing protocol. This extended protocol can maintain vehicles trust at a certain level. Also, experiment analysis is done under different mobility, and malicious attack pattern and comparison is taken out among trust model enabled (proposed scheme), AASR [12] and original AODV. We argue that this phenomenon can also be used with many advance routing protocols for VANET, but the basic theme here is to highlight and apply 3VSL trust model and its accuracy in the proposed scenario. The extended routing table and simulation parameters are given in Tables 2 and 3, respectively.

6.1 Scenario 1: Performance comparison between trust model enabled (proposed scheme), AASR and original AODV (a) effect of mobility setting, (b) varying number of malicious nodes

As shown in Fig. 7*a*, increasing vehicles speed may affect the throughput of CBR traffic and causes it to be degraded or improved in different mobility settings. In this situation, our scheme gets better results than AASR and AODV because it reduces extra routing overhead by exchange of trust information in route packets. The results achieved by our proposed scheme are better than two other routing protocols. Another thing in Fig. 7*b*, AODV has the lower delay than AASR it is due to extra cryptographic processing

in response to packet dropping attacks, while AODV does not care about it and forward packets (malicious) as gets.

Also, in Fig. 7*c*, increasing number of adversaries over time, may affect the throughput of these protocols and cause to be degraded. Since our scheme makes use of trust mechanism and tackle packet dropping attack, by frequently updating the trust counter in each time interval and recalculating the opinion metric, so it outperforms AASR and AODV. From Fig. 7*d*, since original AODV takes these adversaries as regular packets and forwards as gets and does not take any additional action, so it has a lower delay than AASR, which becomes worse in this situation and low mobility. Since our proposed scheme uses the trust relationship between the user vehicles, which helps us to minimise the delay.

6.2 Scenario: 2 Performance comparison between trust model enabled (proposed scheme), and maliciously affected AODV under different attack patterns

In this simulation, we have made a comparison between trust model enabled (proposed scheme), and maliciously affected AODV under the black hole and zigzag attacks patterns. In Fig. 8*a*, we can see that two routing protocols, one is compromised by adversary after $t = 5$ s, so eventually decreases recommendation from neighbours and packet throughput minimises. Here, it is interesting to notice that the semi malicious behaviour from $t = 25$ to $t = 35$ s, as nodes start to misbehave with its neighbours, so their opinion metric updated in terms of getting a bad recommendation thus lower their reputation and trust. After a while as nodes start to behave well they get a good recommendation, thus increasing packet throughput. This behaviour can also be considered as an on–off or zigzag attack. Also in Fig. 8*b*, we can see the effect of black hole attacks, as nodes become thoroughly compromised due to changing route information.

The end-to-end (E2E) delay between our proposed scheme and maliciously affected given in Fig. 8*c*. Here trust model enables (TME) routing is managed to reduce uncertainty during interactions and trust model helps to recognise trustee's and evict malicious peers, thus minimises the delay. On the other hand, the delay in maliciously affected routing increases due to fewer interactions and high uncertainty. Similarly, in Fig. 8*d*, the packet drop ratio is minimum in our proposed scheme.

Table 3 Simulations parameters for secure routing among neighbour vehicles

routing protocol	enhanced AODV
trust assessment	3VSL trust model
simulation area	1000 × 1000 m
total vehicles	50
transmission range	250m
mac protocol	IEEE 802.11
movement model	low mobility
channel bandwidth	2 Mb/s
traffic type	CBR
number of malicious vehicles	0 – 25
vehicle movement speed	0 – 50 km/h

7 Conclusions

In this paper, 3VSL is proposed for accurate trust assessment among neighbour vehicles having arbitrary network topology, a solution to guarantee a simplified trust model in a distributed environment. Conventional cryptographic and PKI based schemes not only ignoring the notion of uncertainty but also requires the central agent to store these public keys or digital certificates. Also, previously proposed solutions are limited to prior suspicion values. However, 3VSL nicely deal prior, and posterior uncertainty exists in trust. 3VSL is also capable to accurately apply to assess trust algorithm in AVT. Further, to prove the accuracy of our proposed scheme, we conduct a numerical and experimental analysis. In numerical analysis, the impact of 3VSL to solve bridge or random network topology is analysed. In the experimental part, we extend widely accepted AODV routing protocol using the proposed trust model, i.e. 3VSL. In different performance evaluations, results support the accuracy of our proposed scheme. We believe that 3VSL framework is a simple solution to assess multi-hop users trust accurately. We will extend our work by considering more advanced simulations platform and routing protocols for VANET combined with 3VSL trust model.

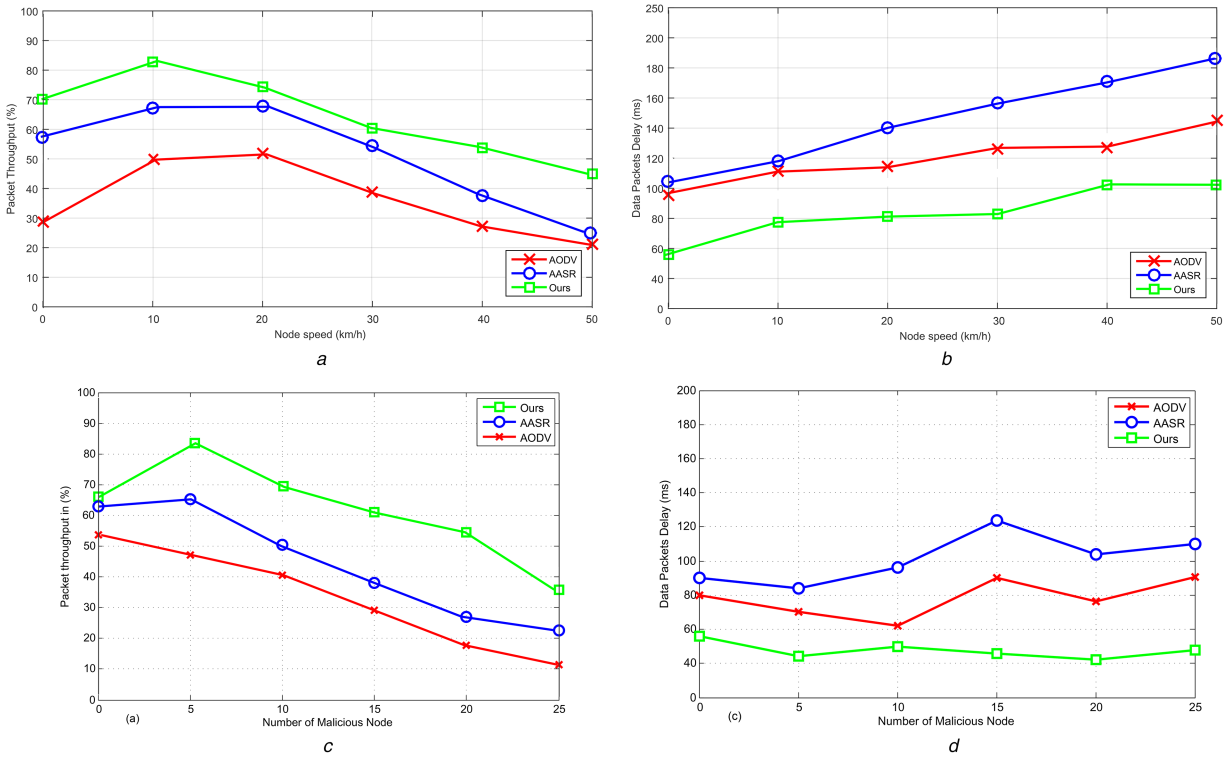


Fig. 7 *Performance analysis among trust model enabled (proposed scheme), AASR and AODV routing protocols under different mobility setting*
(a) Packet throughput, ***(b)*** E2E delay. Performance analysis among trust model enabled (proposed scheme), AASR and AODV routing protocols by increasing number of malicious vehicles, ***(c)*** Packet throughput, ***(d)*** E2E delay

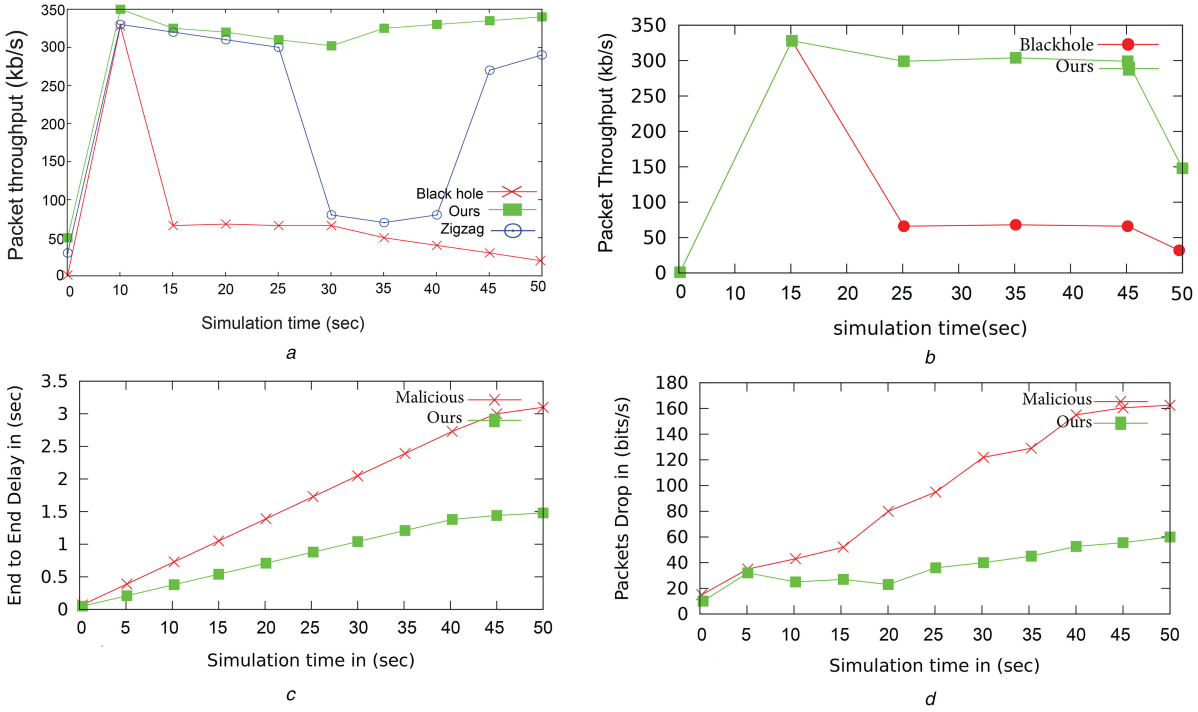


Fig. 8 *Performance analysis under zigzag and black hole attacks with parameters R = 250 m, V = 50 km/h, and malicious vehicles = 25*
(a) Packet throughput (zigzag attack), ***(b)*** Packet throughput (black hole), ***(c)*** E2E delay between malicious and secure routing, ***(d)*** Packets drop between affected and our proposed secure routing

8 Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant U1736216, Grant 61472001, and Grant 61702233, the National Key Research and Development Program Grant 2017YFB1400703

9 References

[1] Mejri, M.N., Ben, O.J., Hamdi, M.: 'Survey on VANET security challenges and possible cryptographic solutions', *Vehi. Commun.*, 2014, **1**, (2), pp. 53–66
[2] Karagiannis, G., Onur, A., Eylem, E., *et al.*: 'Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions', *IEEE Commun. Surv. Tutor.*, 2011, **13**, (4), pp. 584–616
[3] Sun, Y.L., Han, Z., Yu, W., *et al.*: 'A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks'. Proc. IEEE INFOCOM, Barcelona, Spain, 2006, pp. 1–13
[4] Liu, Z., Ma, J., Jiang, Z., *et al.*: 'Lsot: a lightweight self-organized trust model in vanets', *Mob. Inf. Syst*, 2016, **16**, (2), pp. 1–15
[5] Cook, K.S.: 'Trust in society', in Cook, K. (Eds.): '*Russell sage foundation series on trust*' (New York, 2001)
[6] Horng, S.J., Tzeng, S.F., Li, T., *et al.*: 'Enhancing security and privacy for identity-based batch verification scheme in VANETs', *IEEE Trans. Veh. Tech*, 2017, **66**, (4), pp. 3235–3248
[7] Jiang, S., Zhu, X., Wang, L.: 'An efficient anonymous batch authentication scheme based on HMAC for VANETs', *IEEE Trans. Intell. Transp. Systs.*, 2016, **17**, (8), pp. 2193–2204
[8] Yang, Q., Zhu, B., Wu, S.: 'An architecture of cloud-assisted information dissemination in vehicular networks', *IEEE Access*, 2016, **4**, pp. 2764–2770
[9] Liu, G., Yang, Q., Wang, H., *et al.*: 'Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic'. Proc. IEEE INFOCOM, Toronto, ON, Canada, April 2014, pp. 1698–1706
[10] Josang, A., Bhuiyan, T.: 'Optimal trust network analysis with subjective logic'. Proc. Int. Conf. on Emerging Security Information, Systems and Technologies, Washington, DC, USA, August 2008, pp. 179–184
[11] Sohail, M., Wang, L.: '3VSR: three valued secure routing for vehicular *ad hoc* networks using sensing logic in adversarial environment', *Sensors*, 2018, **18**, p. 856
[12] Liu, W., Yu, M.: 'AASR: authenticated anonymous secure routing for MANETs in adversarial environments', *IEEE Trans. Veh. Tech.*, 2014, **63**, (9), pp. 4585–4593
[13] Yang, Q., Wang, H.: 'Toward trustworthy vehicular social networks', *IEEE Commun. Mag.*, 2015, **53**, (8), pp. 42–47
[14] Chen, X., Liangmin, W.: 'A cloud-based trust management framework for vehicular social networks', *IEEE Access*, 2017, **5**, (99), pp. 2967–2980
[15] Hu, H., Lu, R., Zhang, Z., *et al.*: 'Replace: a reliable trust-based platoon service recommendation scheme in vanet', *IEEE Trans. Veh. Tech.*, 2017, **66**, (2), pp. 1786–1797
[16] Govindan, K., Mohapatra, P.: 'Trust computations and trust dynamics in mobile *ad hoc* networks: a survey', *IEEE Commun. Surv. Tutor.*, 2012, **14**, (2), pp. 279–298
[17] Cho, J.H., Swami, A., Chen, I.R.: 'A survey on trust management for mobile *ad hoc* networks', *IEEE Commun. Surv. Tutor.*, 2010, **13**, (4), pp. 562–583
[18] Josang, A.: 'A logic for uncertain probabilities', *Int. J. Uncert. Fuzzi. Knowl. Systs.*, 2001, **9**, (3), pp. 279–311
[19] Li, X., Lyu, M., Liu, J.: 'A trust model based routing protocol for secure *ad hoc* networks'. Proc. Int. Conf. on IEEE Aerospace Conf., MT, USA, March 2004, pp. 1286–1295
[20] Sohail, M., Wang, L., Yamin, B.: 'Trust model based uncertainty analysis between multi-path routes in MANET using subjective logic'. Proc. China Conf. on Wireless Sensor Networks, Tianjin, China, October 2017, pp. 319–332
[21] Sohail, M., Wang, L., Yamin, B.: 'Trust mechanism based AODV routing protocol for forward node authentication in mobile *ad hoc* network'. Proc. Int. Conf. on Mobile Ad-Hoc and Sensor Networks, Beijing, China, December 2017, pp. 338–349
[22] Ren, Y., Zadorozhny, V.I., Oleshchuk, V.A., *et al.*: 'A novel approach to trust management in unattended wireless sensor networks', *IEEE Trans. Mob. Comput.*, 2014, **13**, (7), pp. 1409–1423
[23] Dietzel, S., van der Heijden, R., Decke, H., *et al.*: 'A flexible, subjective logic-based framework for misbehavior detection in V2V networks'. Proc. IEEE World of Wireless, Mobile and Multimedia Networks, Sydney, Australia, 2014, pp. 1–6
[24] Van der Heijden, R.W., Kargl, F., Abu-Sharkh, O.M., *et al.*: 'Enhanced position verification for VANETs using subjective logic'. Proc. IEEE 84th Vehicular Technology Conf. (VTC-Fall), Montreal, QC, 2016, pp. 1–7
[25] Liu, Y., Wang, L., Chen, H.: 'Message authentication using proxy vehicles in vehicular ad ho networks', *IEEE Trans. Veh. Tech.*, 2015, **64**, (8), pp. 3697–3710
[26] Yu, M., Zhou, M., Su, W.: 'A secure routing protocol against byzantine attacks for MANETs in adversarial environments', *IEEE Trans. Veh. Tech.*, 2009, **58**, (1), pp. 449–460
[27] Libert, B., Peters, T., Yung, M.: 'Short group signatures via structure-preserving signatures: standard model security from simple assumptions'. Proc. Advances in Cryptology – CRYPTO, Berlin Heidelberg, Germany, 2015, pp. 296–316
[28] Hafez, A., Xu, Y.: 'Exploiting the beta distribution-based reputation model in recommender system'. Proc. Australasian Joint Conf. on Artificial Intelligence, Canberra, ACT, Australia, November 2015, pp. 1–13
[29] Fung, C.J., Zhang, J., Aib, I., *et al.*: 'Dirichlet-based trust management for effective collaborative intrusion detection networks', *IEEE Trans. Netw. Serv. Manag.*, 2011, **8**, (2), pp. 79–91
[30] 'NS: The Network Simulator'. Available at http://www.nsnam.org/, accessed April 2018