ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue Special 1 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Identifying the Misbehavior Nodes Using Trust Management in VANETs

[I]Muthukumar.S, [II]Karthick Selvan.R
[I]Assistant Professor, Dept. of CSE, Sree Sowdambika College of Engg, Tamilnadu, India
[II]PG Student, Dept. of CSE, Sree Sowdambika College of Engg, Tamilnadu, India

Abstract
In recent years, more and more research has been focusing on trust management of vehicle ad-hoc networks (VANETs) for improving the safeguard of vehicles. However, in these researches, little awareness has been rewarded to the location privacy due to the natural conflict between trust and anonymity, which is the basic safeguard of privacy. Although traffic safety remains the most crucial problem in VANETs, location privacy can be just as important for driver, and neither can be ignored. In this article, we suggest a signal-based trust management method that aims to censor internal attacker from transfer false messages in privacy-improved VANETs. To approximate the reliability and performance of the planned scheme, we conduct a set of simulation under alteration attacks, bogus message attacks and black-hole attacks. The simulation results show that the future system is highly resilient to enemy attacks, whether it is beneath a fixed silent period or random silent period position privacy enhancement scheme.

Keywords
Privacy, Trust Management, Vehicle Ad-Hoc Networks (VANETs)

I. Introduction
With the advance of vehicle-communication technologies, vehicles are now able to communicate with each other via vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) wireless communications. These kinds of communication networks, also called vehicular ad-hoc networks (VANETs), are purported to improve traffic safety while enhancing the road efficiency of the transportation system. However, the raising consciousness of individual's privacy information protection has pushed the protection of location and data privacy as a must be requirement of VANETs. For example, in the USA, in order to comply with privacy protection act or wireless privacy protection act, VANETs have to ensure location privacy information not be disclosed without prior authorization.

To meet above design requirements, the authors of [1]-[4] proposed methods to remove the correlation between locations and identifiers of vehicles, which depend mainly on updating vehicle's pseudo identifiers from time to time. By applying pseudonyms, it becomes more difficult for adversaries to trace vehicles. However, as pseudonym may allow bad ones to hide their identifiers without the risk of being discovered, blindly adopting a privacy-enhancement methodology will raise new safety risks for the whole transportation system. In order to ensure message integrity, message authentication is one of the common adopted methods, such as digital signatures [1] and message authentication codes [5].

A limitation of message authentication is that it can only ensure that messages are sent from legitimate senders, but cannot prevent a legitimate sender from broadcasting bogus or altering the mutable fields of message malevolently. These attacks not only decrease the transportation efficiency, in worst cases, they may cause accidental events that can threaten human life. Take the electronic urgent situation break light as an example, which is used to notify drivers of the rapid deceleration of neighboring vehicles. Bogus EEBL message could cause drivers to decelerate or take sudden evasive action unnecessarily, which might cause a fatal traffic accident, rather than prevent one.

In order to detect the attack behavior, some researches such as misbehavior detection mechanisms [6]-[10] and reputation systems have been proposed. By establishing trust relationships and detecting malevolent behavior in VANETs, these works enable vehicles to distinguish trustworthy vehicles or messages from untrustworthy ones. This can reduce the risk which being misguided by other misbehavior vehicles. We have evaluated the proposed system under fixed silent period (FSP) and random silent period (RSP) schemes through wide simulations. All of the simulations consider alternate attack models, and bogus message attacks. The simulation results show that the proposed signal-based reputation system performs at least 15% outstandingly than the weighted vote method in a location privacy enhanced scheme.

II. Related Work
In this section, we will first briefly review existing works that deal with misbehavior detection and trust-enhancement research on VANETs. Then, we will introduce some misbehavior prevention researches in location privacy-enhanced VANETs, which are related to this paper.

A. Misbehavior Detection in VANETs
In the beginning, misbehavior detections were used to prevent false warning for improving the security of routing protocols in VANETs [6]. With this mechanism, the nodes cheating about their positions in signals can be recognized. Besides, sudden appearance warning (SAW) and maximum beaconing frequency (MBF) [7] are also commonly misbehavior detection mechanisms.

It is proposed a MDS to discover misbehaving or faulty nodes by detecting their deviation from normal behavior. The MDS they proposed can distinguish between two types of misbehaviors: known misbehaviors and data anomalies. In known misbehavior detection, they adopted the position verification methods mentioned above [6]; in data anomalies, their method leveraged the entropy and outlier detection algorithm to detect the malicious event messages. It also proposed a MDS integrated with root-cause analysis [10], in which they first constructed a origin-tree analysis, subsequently they used the logical reduction to indicate the root cause of the misbehavior. It is proposed a framework for misbehavior classification using Waikato environment for knowledge analysis (WEKA), which is efficient in classifying multiple misbehaviors. Besides, also proposed an ensemble approach for misbehavior detection, which can ensemble multiple

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

machine learning approaches. However, performance efficiency is a challenge for their works.

B. Trust Management in VANETs

Trust is a relationship among entities that is based on the observations of historical interactions. A network of nodes with trust relationship can easily distinguish well behavior nodes from misbehavior nodes. In VANETs, such capability can help to ensure the safety of vehicles. There are three models to establish trust: Entity trust model, data trust model, and combined trust model [11]. Entity trust model emphasizes on modeling the trustworthiness of peers. Data trust model focuses on evaluating the trustworthiness of transmission data. Combined trust model uses peer trust to evaluate the trustworthiness of data. In VANETs, entity trust is the traditional notion of trust. It is proposed a distributed entity-centric reputation system named vehicle ad-hoc network reputation system (VARS), which can share trust opinions among neighbor's vehicles in VANETs.

III. Methodology

A. Assumptions

In order to make the proposed protocol and system work properly, we make the following assumptions:

- All on board unit (OBU) are equipped with global positioning system (GPS) with wireless interfaces. The organization time of the OBU are synchronized via GPS.
- OBU use pseudonyms to prevent identify tracking, and all pseudonyms are changed after a short period of time and cannot repeat.
- OBU periodically broadcast single-hop signaling messages, which contain, at least, position, velocity, and headway direction.
- There exist a public key infrastructure (PKI) in VANETs and a fully trustworthy third party that conforms to standards of key management, verification, and revocation.

1. Trust Information Gathering

In general, trust information gathering methods in VANETs can be classified into three major categories: Direct, indirect, and hybrid [3]. Direct trust means that trust information is experimental or obtained by a vehicle itself. Information that is received from neighboring vehicles is the first-hand information. Signal messages and direct received incident messages are mutually types of original-hand information. Indirect trust is also known as subsequent-hand information trust, which is obtained via the recommendations from other vehicles. Hybrid trust combines both direct and indirect trust methods, which can combined the advantages of them and complement their disadvantages. In this article, we adopt hybrid trust by which we obtain direct trust information from beacon messages and direct received event messages and indirect trust from the traditional event message trust recommendation method. In the following context, we give a detailed description of how to compute the direct and indirect trustworthiness of these event messages.

(i). Signal-Based Trust

The main idea of signal-based trust is to estimate and to verify constantly a vehicle location, speed, and drive direction. In this article, cosine similarity [3] is used to compute the angle between the estimated vector and the claimed vector, where vector is the set of vehicle location, speed, and direction values. This angle belongs to the inner product family and is also called the corner metric [2]. The cosine similarity SimCos can be formulated as following:

$$Simcos(\vec{E},\vec{O}) = \frac{\vec{E}.\vec{O}}{|\vec{E}||\vec{O}|} \tag{1}$$

$$= \frac{xExO+yEyO+vEvO}{\sqrt{x^2E+y^2E+v^2E}\sqrt{x^2O+y^2O+v^2O}} \tag{2}$$

Where $\vec{E}$ the estimated vector is based on the latest observations and $\vec{O}$ represents the claimed vector obtained in the latest signal message. Let $\vec{O}=(x_O, y_O, v_O)$ and $E=(x_E, y_E, v_E)$. Both of these vectors consist of three components (x, y, v) are xy coordinates, are v is the velocity of the latest received (1), x_O, y_O are the coordinates of the latest received signal; v_O is the velocity of the latest received signal, and x_E, y_E are the estimated coordinates according to the received signal message before the latest one. (x_E, y_E) can be computed as

(xE,yE)=(tdiff vpre cosθpre+xpre,tdiff vpre sinθpre+ypre) (3)

Where vpre, θpre, (xpre, ypre) are the velocity, headway direction, and xy coordinates of the receive signal message before the latest one, respectively. Furthermore, let tdiff = tlst – tpre, where tdiff is the time difference between the latest timestamp tlst of the latest received signal message and the timestamp tpre before the latest one.

In (4), the signal trustworthiness of a neighboring vehicle is denoted as Tbea, and I is the number of signal that should be taken into consideration. The larger value of I, the longer the time that the signal messages can influence the trustworthiness. In (4), wi is the weight of the last i signal and n is the exponent value. By using n, the importance of the similarity decays over time.

$$Tbea = \frac{\sum_{i=1}^{I} simcos(\vec{Ei},\vec{Oi})(wi)^n}{\sum_{i=1}^{I}(wi)^n} \tag{4}$$

(ii). Event-Based Trust

For public safety, vehicles broadcast event-driven warning messages, such as approaching emergency vehicle warnings, SOS services, EEBLs, and post-crash notifications (PCNs) [3], to neighboring vehicles. In this article, we call such an event driven warning messages as "event-based message". Let Mevt = {IDs -- MIDevt -- Tpevt -- MSevt -- Levt -- tevt} represent an event-based message, where IDs is the pseudo identifier of the message sender S; MIDevt is the message identifier; TPevt is the message type, such as the public safety applications mentioned in section I; MSevt is the description of the event; Levt is the position of the event; and tevt is a positive integer, representing the event time, and -- represents the concatenation of information.

(iii). Direct Event-Based Trust

In order to compute the trustworthiness of a direct event-based message, we propose a position-based and movement-verification mechanism. By this mechanism, a receiving vehicle is able to evaluate the trustworthiness of the sender vehicle by analyzing both the received event messages and the signal messages from a vehicle.

$$SimTan(\vec{E},\vec{R}) = \frac{\vec{E}.\vec{R}}{|\vec{E}|^2+|\vec{R}|^2-\vec{E}.\vec{R}} \tag{5}$$

Where $\vec{E}$ the vector of the location information is estimated from the signal message and $\vec{R}$ is the vector of the location from the received event message. In order to verify event-message plausibility and maintain trustworthiness, (6) is used to compute the composite direct event trust Tdevt, where Δd denotes the distance between the message transmitter, and Δt denotes the time delay between the event message timestamp and the receiver's current timestamp. If Δd is larger than maximum transmission distance Dmax or Δt is greater than maximum event message delay Tmax, then the trustworthiness of event message Tdevt will be set to zero. After passing the plausibility verification, Tdevt will be assigned by the composite value of the cosine similarity and Tan similarity with the weight value α.

$$Tdevt = \begin{cases} 0, & if\ \Delta d > Dmax\ or\ \Delta t > Tmax \\ \alpha SimTan + (1-\alpha)Simcos, & otherwise \end{cases} \quad (6)$$

(iv). Indirect Event-Based Trust

When message receiver establishes trust relationships through the recommendation of further vehicle, the trustworthiness between the sender and receiver should not be more than the trust value between the receiver and the forwarder, as well as the trust value between the sender and the forwarder. The indirect trustworthiness of the incident message Tevt is calculating according to (7).

$$Tevt(e) = \begin{cases} Tevt, & if\ e\ is\ direct\ event \\ \min(Topn,\ Tdevt), & otherwise \end{cases} \quad (7)$$

B. Reputation and Trust Compositing

The incident reputation value Trep of a vehicle can be computed as

Trep(t)=βTevt(t)+(1-β)Trep(t-1) (8)

Where (1 - β) is the weighted value for the previous reputation value. After a vehicle computes the incident trust value Tevt, it update the earlier reputation value in order to take the historical event trust value into consideration.

Tcom is the composite trustworthiness of the received incident message, and Tcom is calculated as

Tcom = Tbea wbea + Tevt wevt + Trep wrep (9)

1. Trustworthiness Combining

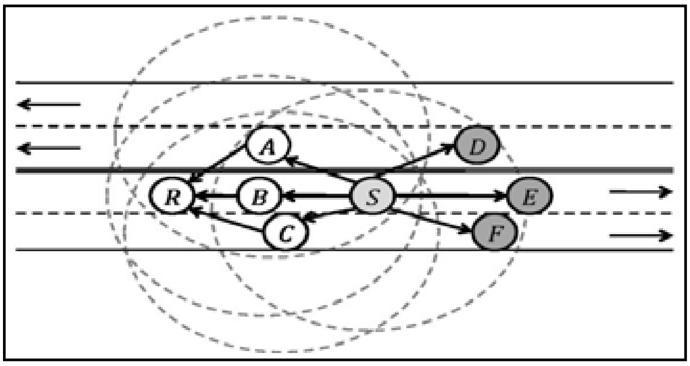

Fig. 1: Combining the Trustworthiness for the Event Messages

When a vehicle receives a direct event message or an indirect event message opinion transmitted from multiple vehicles, it needs to find an effective solution to combine the received opinions and then to determine the overall trustworthiness of this event message. Take Fig. 1 as an example: Vehicle S broadcasts a multi-hop event message, and vehicles A, B, C, D, E, and F are in the transmission radius at the same time. When these vehicles receive this event message, they will forward this event message to their vicinity vehicles, together with their opinion about this event message.

Algorithm : Decision making algorithm

Input : Trust set T; Event message msg_i transmitted from vehicle i; set of received message M;

Output : Decision D

$\Delta t \leftarrow t_{recv} - t_{first}$;

$M \leftarrow M \cup msg_i$;

$T^i_{com} \leftarrow T^i_{bea} \times w_{bea} + T^i_{evt} \times w_{evt} + T^i_{rep} \times w_{rep}$;

$T \leftarrow T \cup T^i_{com}$;

if $|M| \geq M_{max}$ and $\Delta t \geq t_{wait}$ **then**

  $T^{sup}_{ds} \leftarrow \bigoplus_{n=1}^{|M|} m_n(H_{sup})$;

  $T^{deny}_{ds} \leftarrow \bigoplus_{n=1}^{|M|} m_p(H_{deny})$;

  if $T^{sup}_{ds} > T_{thld}$ **then**

    $D.opn \leftarrow accept$;

    $D.trust \leftarrow T^{sup}_{ds}$;

  else

    $D.opn \leftarrow deny$;

    $D.trust \leftarrow T^{deny}_{ds}$;

return D;

Fig. 2: Decision Making Algorithm

In this paper, we adopt the belief value in DST as the trust value. The combined trust value Tds corresponding to an event is represented as in (10).

$$Tds(i) = \bigoplus_{n=1}^{|M|} mn\ (Hi) \quad (10)$$

Where M is the set of received event messages and |M| is the number of event messages in M. In the example of Fig. 1, for vehicle R, set M contains {msg1, msg2, msg3}, which are transmitted from vehicle {A, B, C}, respectively.

$$m1(Hi) \oplus m2(Hi) = \frac{\sum_{q,r:\ Hq \cap Hr = Hi} m1(Hq)m2(Hr)}{1 - \sum_{q,r:\ Hq \cap Hr = \emptyset} m1(Hq)m2(Hr)} \quad (11)$$

If the opinion of the event message is trustworthy, and the trustworthiness of this vehicle n is Tn, then its probability assignment will be:

mn(T) = Tn,mn(~T) = 0,mn(Ω) = 1-Tn

IV. Proposed System

In a proposed system, it is used to Trust Authority, which is used for overall maintaining the number of nodes. If one node can transfer the data in a VANET network then it can calculate the time period. If new nodes can entry in the VANET network then it can generate the private key of that node. Therefore that new node can transfer the data in the network then it can generate the session key. In a proposed system, it can detect the misbehavior node then it can be prevent that node. In this system, the cluster head node can send the data correctly or not correctly in all nodes cannot be identified by the server. It also proposed a trust authority can be placed in between the server and VANET network. Detect the number of attacks is easily and less.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

V. Performance Evaluation

A. Adversary Model

In this paper, we consider an adversary to be a vehicle equipped with an OBU in a certain area of the VANET. The enemy can actively participate in the network and violate the integrity of messages, such as by broadcasting or forwarding malicious messages. Focused attack models are listed below [9].

- Alteration attacks (Aalt): Due to the protection of event message signature, alteration attacker cannot alter the non mutable fields which signed event message. However, malicious attacker still can modify the mutable opinion and opinion trustworthiness fields of a multi-hop event messages, then forward the event message.
- Message suppression attacks (ADoS): Malicious vehicles can drop received multi-hop event messages that suppress legitimate alerts from further propagation. This is also called black hole attack [4]. However, wireless bandwidth jamming is beyond the scope of this article and has been excluded.
- Bogus message attacks (Abog): Malicious vehicles can generate and broadcast malicious event messages to other vehicles in the vicinity.

B. Evaluation

Table 1: Parameters used in this Simulation

Parameter	Value
MAC layer	IEEE 802.11
Propagation	TwoRayGround
Radius	250 m
Road	Two directions: Each 3 lanes
Signal TTL	1 hop
Incident TTL	5 hops
Map	Marattan street map
Map size	5x5 street blocks
Each blocks	300 m2
Velocity	0_27 m/s
Average velocity	11.26 m/s

In order to evaluate the performance of the proposed system under alteration attacks, message suppression attacks, and bogus message attacks, Table 2 shows the probability parameters for the possible decisions. After the simulation ends, the decision results of the misbehaving vehicles are excluded. When a vehicle receives an event message, the system computes the trustworthiness of the received event message and decides whether the message is responsible or not. During the simulation, both normal and attack messages are transmitted in the VANETs.

Table 2: Probability notations for the possible decisions under various adversary models (p, q, r, s, t, u, v, w indicate different circumstances)

	Decisions	
Circumstances	Trustworthy	Untrustworthy
Normal message (Nor)	TN p	FP p
Bogus message (A_{bog})	FN q	TP q
Nor + A_{alt}	TN r	FP r
Nor + A_{DoS}	TN s	FP s
Nor + A_{alt} + A_{DoS}	TN t	FP t
A_{bog} + A_{alt}	FN u	TP u
A_{bog} + A_{DoS}	FN v	TP v
A_{bog} + A_{alt} + A_{DoS}	FN w	TP w

As shown in Table 2, if a vehicle sends normal event messages under various attack models, such as alteration attacks or DoS attacks, then the decisions are true negative (TN) opinions when the receiving vehicle decides these event messages are trustworthy. In contrast, if the receiving vehicle sends out its opinion and indicates that the original normal event messages are untrustworthy, then this decision is a false positive (FP) decision. The calculation of TN and FP opinions under different attack models is performed as in (12).

$$TN = \sum_{i \in \{p,r,s,t\}} TNi, FP = \sum_{i \in \{p,r,s,t\}} FPi \quad (12)$$

$$FN = \sum_{i \in \{q,u,v,w\}} FNi, TP = \sum_{i \in \{q,u,v,w\}} TPi \quad (13)$$

After determining TN, TP, FN and TP, we use these parameters to obtain both precision rate (P) and recall rate (R), as shown in (14) and (15), respectively. In this article, we adopt F-measure (denoted as F) [4], as shown in (16), to calculate the overall performance of the proposed scheme. It is significant to evaluate precision and recall together, because of the easiness of optimizing separately. The F-measure is a weighted combination of accuracy, with its value from 0 to 1. However, it is noted that the F-measure does not capture the true negative rate into account.

$$P = \frac{TP}{TP + FN'} \quad (14)$$

$$R = \frac{TP}{TP + FP'} \quad (15)$$

$$F = \frac{2PR}{P + R^2} \quad (16)$$

V. Simulation Results

In this section, we evaluate the performance of the proposed scheme under the following three stringent adversarial models: Alteration attacks, message suppression attacks, and bogus message attacks. In addition to the adversarial models, we also compare location privacy enhancement scheme FSP with RSP. All of the above evaluation results will be shown in the following sections. A.

A. Effect of the Misbehavior Vehicle Rate

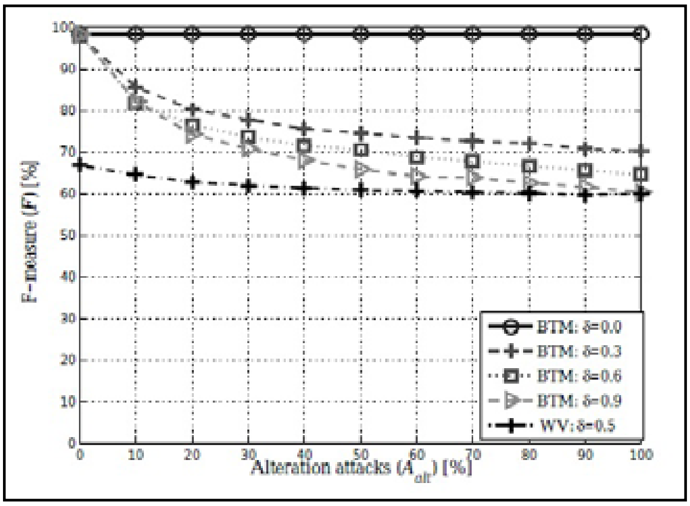

Fig. 3: Different rates of misbehavior vehicles (η=0, ω=1).

B. Effect of Bogus Messages

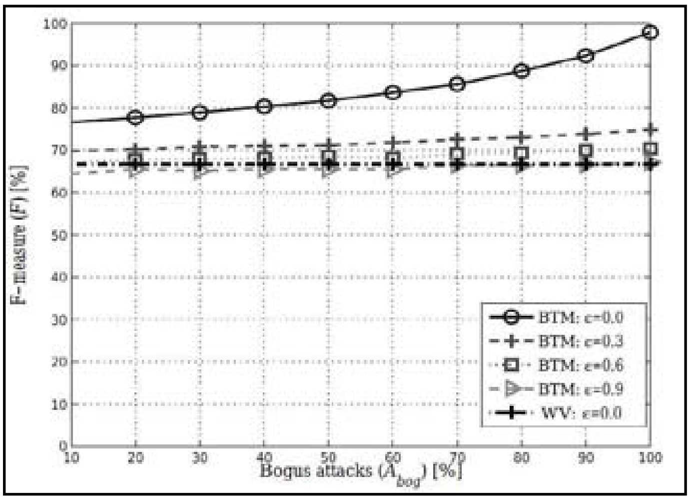

Fig. 4: Different bogus message attack rates (δ = 0.5, η = 0).

C. Effect of Trust Opinion Propagation

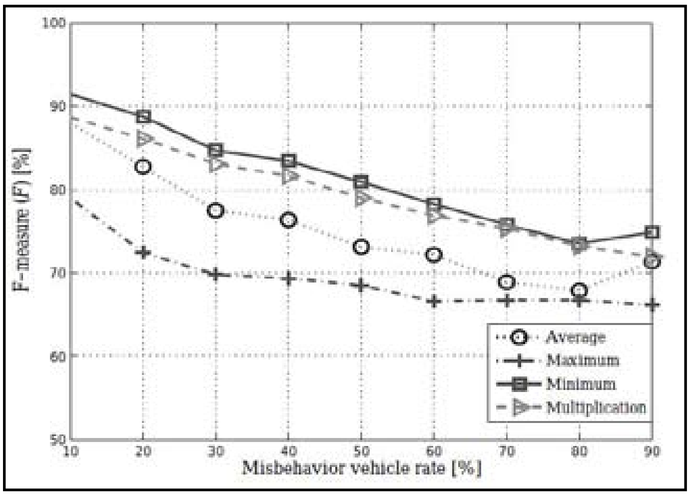

Fig. 5:Trust-propagation methods vehicles (η=0, δ=0.5, ω=1)

D. Detection Delay

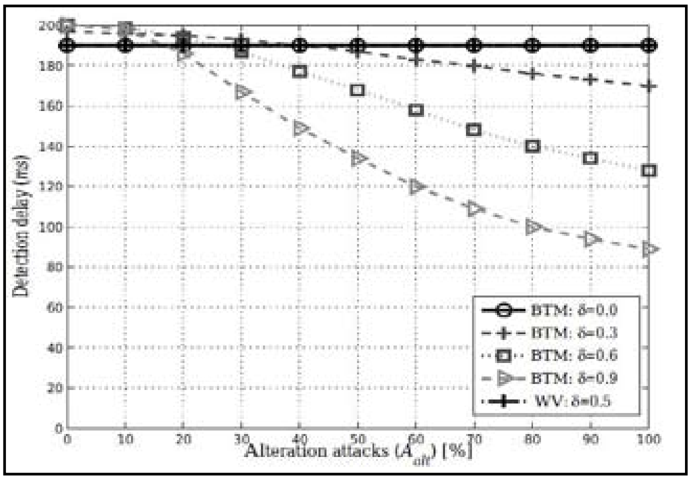

Fig. 6: Detection delay in different attack models (η=0, ω=1)

To see the effect of the misbehavior vehicle rate, we experiment with different misbehavior vehicle rates and various alteration attack rates. In addition to alteration attack rates, we also take bogus message rates into account in this simulation. Fig. 3 shows that the proposed system can perform better than the WV mechanism. Even when misbehavior vehicle rate is 90 percent, the result is still better than that of the WV mechanism with a 50 percent misbehavior vehicle rate.

We mentioned four methods of trust opinion propagation, namely, multiplication, averages, maximums, and minimums. In order to illustrate the difference between these types of indirect trustworthiness propagation methods, we evaluate these four methods respectively. In Fig. 5, we can see that the minimum trust opinion propagation method is the most suitable one for our proposed system. Although the multiplication method is the most popular method and has been used in many trust-establishment schemes, the minimum method can perform better than others in a DST trust combining approach.

In addition to the detection accuracy of the proposed system, detection delay is also a major issue in evaluation. In order, to evaluate the detection delay of our proposed system, we experiment with different misbehavior vehicle rates with various alteration attack rates. As shown in Fig. 6, we observe that the detection delay of the proposed trust system is not influenced by the detection model. When alteration attack rate and misbehavior vehicle rate rose over 90 percent, the detection delay becomes lower than 100 millisecond.

VI. Conclusion

In this paper, we propose a novel trust management aiming to thwart malicious attackers in location privacy-enhanced VANETs. In this system, a vehicle can utilize not only direct or indirect event messages, but also signal messages to construct trust relationships in order to distinguish trustworthy event messages. The simulation is highly resilient to three attack models. Another important contribution of our scheme is that it is suitable for both FSP and RSP location privacy-enhanced schemes. In our evaluation, the average F-measure value of the proposed system is 18% greater than WV method in FSP scheme and 15% in RSP scheme. Thus, we can conclude that the proposed trust-management system cannot withstand trust attack models, but also is viable for location privacy-enhanced schemes.

Vol. 2 Issue Special 1 Jan-March 2014
ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

In the future, we intend to improve the detection rate of the proposed system and to evaluate the performance of the proposed scheme with different vehicle densities and average velocities. Moreover, making comparison with other trust management system will be another important investigation topic in our future work. We also plan to investigate countermeasures to alteration attacks and extend our system to defend against other type of attacks in the future.

References

[1] F. Dotzer, *"Privacy issues in vehicular ad hoc netbworks," in proc. PETS, vol. 3856, Springer Berlin Heidelberg, 2006, pp. 197-209.*

[2] T. Leinmuller, E. Schoch, and F. Kargl, *"Position verification approaches for vehicular ad hoc networks," IEEE Wireless Commun., vol. 13, pp. 16-21, Oct. 2006.*

[3] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, *"Detecting misbehaviors in VANET with integrated root-cause analysis," Ad Hoc Netw., vol. 8, no. 7, pp. 778-790, 2010.*

[4] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, *"Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559-573, 2010.*

[5] J. Grover, V. Laxmi and M. Gaur, *"Misbehavior detection based on ensemble learning in VANET advanced computing," in Proc. ADCONS, vol. 7135, Springer Berlin Heidelberg, 2012, pp. 602-611.*

[6] J. Gorover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, *"Machine learning approach for multiple misbehavior detection in VANET," in Proc. ACC, vol. 192, Springer Berlin Heidelberg, 2011, pp. 644-653.*

[7] Z. Huang, S. Ruj, M. Cavenaghi, M. Stojmenovic, and A. Nayak, *"A social network approach to trust management in VANTs," Peer-to-Peer Netw. Appl., pp. 1-14, 2012.*

[8] X. Zhuo, J. Hao, D. Liu, and Y. Dai, *"Removal of misbehaving insiders in anonymous VANETs," in Proc. ACM MSWIM, 2009, pp. 106-115.*

[9] R. Schmidt, T. Leinmuller, E. Schoch, F. Kargl, and G. Schafer, *"Exploration of adaptive signaling for efficient intervehicle safety communication," IEEE Network, vol. 24, no. 1, pp. 14-19, 2010.*