RGTE: A Reputation-based Global Trust Establishment in VANETs

Xiaoqing Li
The State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an, Shaanxi 710071, P.R. China
E-mail: xqli@mail.xidian.edu.cn

Jicheng Liu
The State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an, Shaanxi 710071, P.R. China
E-mail: ljc723@126.com

Xuejun Li
The State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an, Shaanxi 710071, P.R. China
E-mail: aluckydd @mail.xidian.edu.cn

Weiying Sun
The State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an, Shaanxi 710071, P.R. China
E-mail: s_w_y888@126.com

***Abstract*-In recent years Trust Management has become a main method to ensure the security of vehicular ad-hoc networks (VANETs). However, most of the existing trust establishment approaches cannot handle the rapidly changing environment of VANET appropriately. In this paper, we propose a Reputation-based Global Trust Establishment scheme (RGTEs). The scheme introduces a solution to share the trust information in VANET safely by applying statistical laws, which makes it more efficient and accurate to establish trust in rapidly changing environment. Moreover, we detect a bad node by dynamic threshold according to real-time reputation status of the network. Analysis shows that RGTEs is more effective in confidence-building, security assurance and adaptability.**

Keywords: VANET; Trust management; Dynamic threshold;

I. INTRODUCTION

With the rapidly development of VANET, it is of great significance to ensure the security of the distributed network. Generally speaking, most of the nodes in VANET are cooperative and friendly. However there are still some malicious or selfish nodes that will threaten the stability of the network[5,14,15]. Just as we cooperate with each other under the conception of trust in human society, trust establishment scheme is introduced to VANET to help normal nodes make right choice and constrain harmful behavior of bad ones. As a result we encourage all nodes in VANET to be active in cooperation and punish those who may jeopardize the network.

In recent years, a great deal of work[3,6,10,11,14] has been done on trust management in VANET. All of those proposals can generally be classified into the following three categories[1,16]: data rust, entity trust and combination of entity trust and data trust.

- *Data trust:* those systems[2,5,6] aim to build trust on every message generated by nodes in VANET. According to the trust of a message a node can decide to accept it or not. Some data trust systems[4] need a knowledge model of VANET so that a node can evaluate the trust of a message by the patterns stored in advance. Actually it is difficult to build such an intelligent and dynamic database. In other systems[5,6] a node tends to consult the suggestion of nodes which have got the message or to gather suggestion from its neighborhoods. Such a voting like model makes a node vulnerable to collusion attack. Moreover, it is impracticable to verify the reality of the message as with rapidly changing environment.
- *Entity trust:* In most of the trust management schemes focused on entity trust[7,9,12], every node maintains the trust of the others individually. As is known that the average speed of vehicles can be as high as 80km/h in VANET. The communication time between two nodes is very short and a node has little chance to meet the current node again[13]. Since the behavior of a node can be changing all the time, a node builds trust respectively in those approaches is not reasonable. Some schemes try to solve the problem partly by introducing the concept of recommend trust. However, a node accepts recommend trust from others directly may be unsafe. For example, some malicious nodes may collude with each other to fool a normal one by recommending false trust. Another problem of those approaches is that reputation level of the whole network is changing constantly. A single node cannot handle the real-time reputation status of all nodes in the network while trust is processed individually. As a result malicious nodes cannot be detected precisely according to a permanent threshold.
- *Combined trust:* In those systems[3,14,17] a node may not treat suggestion from other nodes equally when calculating the trust of a message. If a node has a higher reputation, its suggestion may be more valuable than others. It sounds more reasonable to get a right trust for a message in this way. However it fails to propose a practical way to build and update the reputation of nodes.

Given the defects of exist schemes analyzed above, we propose a Reputation-based Global Trust Establishment scheme (RGTE). In our scheme we take into consideration three important factors which include properties of VANET, security and efficiency in trust-building. Nodes in RGTE share its trust with others by sending trust messages to Reputation Management Center(RMC). RMC is an authentic infrastructure who collects trust from all legitimate nodes in VANET. Before calculating the reputation of a node, RMC should filter out suspicious trust messages by statistical regularity. With the help of RMC any node in network especially new nodes can acquire up to date trust information of the

978-0-7695-4988-0/13 $26.00 © 2013 IEEE
DOI 10.1109/INCoS.2013.91

whole network safely.

The remainder of this paper is organized as follows: In section II we present system assumption and system model. Section III describes the RGTE scheme in detail. We analyze the proposed scheme in section IV and give a conclusion in section V.

II. RELATED WORK

A. System assumptions

Based on the properties of VANET, The assumptions of our scheme are presented as follows:

1) VANET is on a large-scale and most of its nodes behave in good manner.

2) The average speed of a node may be very high.

3) Sometime the distribution of nodes is so sparse that a node has few adjacent nodes to consult.

4) Nodes in our scheme are equipped with sensors so they can detect status of nodes around them.

B. Trust information protection

The trust information sent by node is vulnerable to adversary as VANET takes use of wireless communication. It is critical to ensure the integrity, confidentiality and Non-repudiation of the trust information. Otherwise, it may be tampered or falsified by malicious node. We choose PKI as the solution to ensure information security. Every node sends a request to RMC and receives a pair of keys (P_i, S_i) before it gets access to the network. The detail descriptions are shown in Tab.1.

TABLE 1. Related notations used in RGTE

Name	Description
ID_i	Unique identity of node i
P_i/P_{RMC}	Public key of node i/RMC
S_i/S_{RMC}	Private key of node i/RMC
$\mathcal{E}_{P_i}(*)$	Encrypt message with key P_i
$\mathcal{D}_{S_i}(*)$	Decrypt message with key S_i
$sig_{S_i}(*)$	Sign with private key S_i
$h(*)$	Hash function

C. Central limit theorem(Lindeberg-Levy)

Suppose $\{X_1, X_2, X_3, \cdots, X_n\}$ is a sequence of independent and identically distributed random variables with $E(X_i) = \mu$ and $Var(X_i) = \sigma^2 < \infty, i = (1,2,3,\cdots,n)$ Then as n approaches infinity, the random variables $\sqrt{n}(\left(\frac{1}{n}\sum_{i=1}^{i=n} X_i\right) - \mu)$ converge in distribution to a standard normal distribution $N(0, \sigma^2)$:

$$\sqrt{n}(\left(\frac{1}{n}\sum_{i=1}^{i=n} X_i\right) - \mu) \xrightarrow{d} N(0, \sigma^2)$$

In our scheme the trust of node ID_i is calculated respectively with the same algorithms by all nodes involved. Theoretically speaking, we can treat those trusts as independent and identically distributed random variables. Obviously it follows a normal distribution according to the theory while VANET is on a large-scale.

D. System model

Direct trust $T_D(i,j)$ means node i calculates its trust on node j directly through the data it senses from node j. Generally speaking, a direct trust has a direction and $T_D(i,j) \neq T_D(j,i)$. When node i makes use of its previous direct trust to make decision or gain its current direct trust, the direct trust should be regarded as experience trust or historical trust $T_E(i,j)$. By the way, $T_E(i,j)$ has a direction as well.

Reputation of node i noted as $\mathcal{R}(i)$ stands for global trust of node i, which is recommended by authentic center RMC. On some degree we can take it as unified trust of all nodes on node i. Related symbols are indicated by Tab.2.

TABLE 2. Related notations used in RGTE

Name	description
$T(*)$	Trust value in range of [0,1]
$\mathcal{R}(*)$	Reputation value in range of [0,1]
$T_D(i,j)$	Direct trust value of node i on node j
$T_E(i,j)$	Experience trust or historical trust of node i on node j
$\mathcal{R}(i)$	Reputation of node i

With the equipment of a sensor any node in our system has ability to sense the environment around it. A normal node is supposed to monitor all nodes within its communication range. As Fig.1 illustrates, trust messages are translated to nearest road side unit (RSU) in the way of vehicle to infrastructure (V2I) or vehicle to vehicle (V2V). RSU verifies the validity of the message and forwards it to RMC through a secure link. RMC takes charge of generating reputation objectively and response to reputation query from nodes.

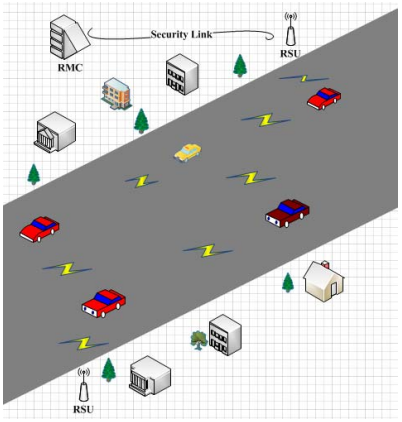

Figure 1. System model of RGTE

III. REPUTATION-BASED GLOBAL TRUST ESTABLISHMENT SCHEME

In this section we will show how RGTE scheme works. Fig.2 below tells us the basic process of interaction among node, RSU and RMC briefly.

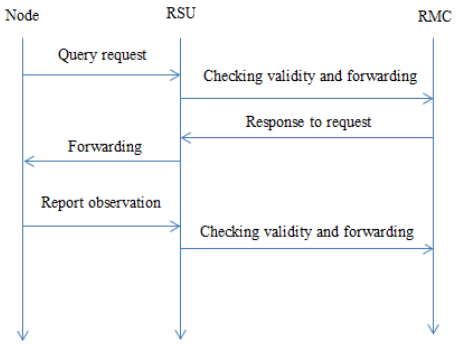

Figure 2. Process of communication

More detailed formulates and algorithms are presented as follows:

A. *Information gathering and processing*

The elements of trust vector play an important role in determining trust value correctly. Taking into consideration properties of VANET, feasibility and security, we define our attributes vector as follows:

$$\mathrm{T}_{attr}{}^{T} = \{Fi, Td, Af, At, Ss, Vt\}$$

Meanwhile, the contribution of different attributes to trust calculating varies greatly. We give another vector of correction factors as weight of each attribute mentioned above:

$$\mathrm{W}_{x}{}^{T} = \{\alpha_{Fi}, \alpha_{Td}, \alpha_{Af}, \alpha_{At}, \alpha_{Ss}, \alpha_{Vt}\}$$

and

$$\alpha_{Fi} + \alpha_{Td} + \alpha_{Af} + \alpha_{At} + \alpha_{Ss} + \alpha_{Vt} = 1$$

Attributes used above are shown in Tab.3.

TABLE 3. Related notations used in RGTE

name	Description
Fi	Forwarding index
Fd	Forwarding delay
Af	Active frequency
At	Alive time
Ss	Signal strength
Vt	Speed of vehicle

Once a node detecting a new node within its communication range, firstly it searches its local reputation list gained from RMC before. If it fails to find a valid record of the new node, the node will send a query request to RMC and update its local reputation list. With the help of RSU, RMC can predict which of the nodes the node may encounter intelligently once accepting a request from a node. That RMC just needs to send back corresponding reputation list instead of the whole list spares communication bandwidth efficiently.

A normal node will calculate direct trust $T_D(i,j)$ of nodes within its communication range in every Δt time:

$$T_D(i,j) = T_{attr}{}^{T} * W_x$$

The experience trust expression is given below:

$$T_E(i,j)_n = T_E(i,j)_{n-1} + \frac{(T_D(i,j)_n - T_D(i,j)_{n-1})}{|T_D(i,j)_n + T_D(i,j)_{n-1}|} * \beta$$

Where β is a coefficient whose default setting can be 2. $T_E(i,j)_{n-1} = R(j)$ while $n = 1$.

About every $\Delta T \geq k * \Delta t$ (k is a constant) node i reports its experience trust observation to RMC. Some nodes may stay within communication range of node i less than ΔT time due to complicate road environment. As for this case, node i will not report its experience trust until it is ΔT. We define encrypted message $\mathcal{M}$ as:

$$m' = T_E(i,j) \parallel T_E(i,k) \parallel \cdots \parallel timestamp$$

$$\mathcal{M} = \mathcal{E}_{P_{RMC}}(\mathrm{ID}_i \parallel m' \parallel h(m') \parallel sig_{S_i}(\mathrm{ID}_i \parallel m' \parallel h(m')) \parallel P_i \parallel n)$$

B. *Message validity checking*

For simplicity, we let RSU share the same pair of keys with RMC. When an RSU receives a message from normal node, it decrypts the message with its private key S_{RMC} and checks over the validity of the message according to signature attached. The detailed processes are shown as follows:

Decryption:

$$\mathcal{M}' = \mathcal{D}_{S_{RMC}}(\widetilde{\mathcal{M}}) = \mathrm{ID}_i \parallel \tilde{m} \parallel h(*) \parallel sig_{S_i}(*) \parallel P_i \parallel n$$

Verify signature:

$$\mathrm{ID}_i \parallel \tilde{m} \parallel h(*) = \mathcal{E}_{P_i}\left(sig_{S_i}(*)\right)$$

Confirm integrity:

$$h(\tilde{m}) = h(*)$$

At last, if the timestamp attached is still valid, RSU forwards the message to RMC through a secure link. Otherwise the message will be ignored.

C. *Reputation maintaining*

In a VANET of n nodes, all of the messages collected by RMC are stored in a $n * n$ matrix as follows:

$$\begin{array}{cccccccc}
ID & ID_1 & ID_2 & ID_3 & \cdots & ID_i & \cdots & ID_n \\
ID_1 & 1 & T_E(1,2) & T_E(1,3) & \cdots & T_E(1,i) & \cdots & T_E(1,n) \\
ID_2 & T_E(2,1) & 1 & T_E(2,3) & \cdots & T_E(2,i) & \cdots & T_E(2,n) \\
ID_3 & T_E(3,1) & T_E(3,2) & 1 & \cdots & T_E(3,i) & \cdots & T_E(3,n) \\
\vdots & \vdots & \vdots & \vdots & \ddots & \cdots & \cdots & \vdots \\
ID_i & T_E(i,1) & T_E(i,2) & T_E(i,3) & \vdots & 1 & \cdots & T_E(i,n) \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
ID_n & T_E(n,1) & T_E(n,2) & T_E(n,3) & \cdots & T_E(n,i) & \cdots & 1
\end{array}$$

If $i = j$, $T_E(i,j)$ stands for the trust of node i on itself. Actually we can initialize $T_E(i,j)$ to 1. It is obvious that the i_{th} column contains all experience trust on node i.

RMC calculates and updates the reputation of node i about every $\Delta\tilde{T}$ time. The detailed processes are shown below:

Average value of experience trust:

$$\mu_i = \overline{T_E(k,i)} = \frac{1}{n-1}\sum_{k=1,k\neq i}^{k=n} T_E(k,i).$$

Standard deviation of experience trust:

$$\sigma_i = \sqrt{\frac{1}{n-1}\sum_{k=1,k\neq i}^{k=n}(T_E(k,i)-\mu_i)^2}$$

According to Central limit theorem and the assumption that most of the nodes in VANET are honest, we judge experience trust that meets the condition below as validity.

$$T_E(*,i) \subset [\mu_i - \gamma\sigma_i, \mu_i + \gamma\sigma_i]$$

Where γ is a constant and its default value is 3.

Let S-sets contains all of the experience trusts that satisfy the condition above, we can get another average value with security ensured.

$$\tilde{\mu_i} = \frac{1}{n-1}\sum_{k\in S} T_E(k,i)$$

$$\mathcal{R}_D = \tilde{\mu_i}$$

Reputation calculation and update:

$$\mathcal{R}(i)_n = \mathcal{R}(i)_{n-1} + \frac{\mathcal{R}_D - \mathcal{R}(i)_{n-1}}{|\mathcal{R}(i)_{n-1} + \mathcal{R}_D|} * \theta$$

Where θ is a coefficient and its default value is 2.

D. Dynamic threshold determination

The reputation list is presented in Tab.4.

TABLE 4. Reputation list model

ID_i	$\mathcal{R}(i)$	TTL	STATUS

TTL means this reputation list has a lifetime. A node can easily check whether a reputation list is out of valid by the value of TTL.

RMC supervises reputation level status every time it updates the reputation of the whole network. Under the assumption that most of the nodes in VANET are normal, we define top 95 percent of nodes are normal and set the status as normal. The rest of the nodes are considered as untrustworthy and their status attribute is set as malicious. If a node finds out that the status of another node within its range is labeled as malicious, it tries not to communicate with the malicious node. As the reputation level changes, the threshold changes as well. In this way, nodes in VANET can detect a bad node accurately and keep important data out of malicious nodes.

IV. ANALYSIS

RGTE scheme makes it more convenient for nodes to get the reputation of any node through V2I or V2V communication. With the assistance of RSU, the frequency of nodes querying reputation information can be dramatically decreased. As a result, RGTE makes it more efficient for nodes build trust on each other without costing too much bandwidth.

Security is an important aspect to which RGTE has paid great attention particularly. RGTE give effective solutions to the three common threatens which are generally mentioned in recent researches.

1) Selfish Attack

If a node behaves lazy or drops dada it received from other nodes deliberately, its adjacent nodes can detect the event immediately. In a short time, the reputation of malicious nodes decreases to quite a small value. Eventually, all normal nodes avoid communication with attackers.

2) Collusion Attack

In RGTE scheme, node does not receive recommend trust directly from other nodes. RMC works as a medium between normal node and adversary which makes it impossible for attackers fool a normal node maliciously. Experience trusts collected by RMC are filtered by particular algorithm before reputation calculating to exclude abnormal data. Hence collusion attackers cannot make it in RGTE scheme.

3) On-Off Attack

Algorithms to generate reputation of a node is designed to make sure that good behavior increase reputation slowly while bad behavior decrease reputation quickly. We can also modify the constant factor according to real status of network to expel adversary out of network within a less time.

V. CONCLUSION AND FUTUER WORK

From the analysis of RGTE scheme, we can draw a conclusion that RGTE scheme has advantage in confidence-building, security assurance and high adaptability in rapid changing environment of VANET.

In our future work we will focus on improving the algorithms to get a more reasonable dynamic threshold and complete the strategy of distinguishing malicious nodes. We will finish the relative simulation work as well.

ACKNOWLEDGMENT

We are grateful to the anonymous referees for their invaluable suggestions. This work is supported by the National Key Basic Research and Development Plan Program of China (973 Program) (No. 2012CB316100) and the Fundamental Research Funds for the Central Universities (No. 5051201011).

REFERENCES

[1] Shuo Ma, Ouri Wolfson and Jie Lin. A Survey on Trust Management for Intelligent Transportation

System. IWCTS'11, Nov 1, 2011.

[2] Aifeng Wu, Jianqing Ma and Shiyong Zhang. RATE: A RSU-Aided Scheme for Data-CentricTrust Establishment in VANETs. IEEE 2011.

[3] Florian Dotzer, Lars Fischer and Przemyslaw Magiera. VARS: A Vehicle Ad-Hoc Network Reputation System. IEEE 2005.

[4] Chen, C., Zhang, J., Cohen, R. and Ho, P.-H. A Trust Modeling Framework for Message Propagation and Evaluation in VANETs. ITCS, 2010.

[5] David Antolino Rivas and Manel Guerrero-Zapata. Chains of Trust in vehicular networks: A secure Points of Interest dissemination strategy. Ad Hoc Networks 10 (2012) 1115–1133.

[6] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," Technical Report, LCA-REPORT-2007-003, 2007.

[7] T. Huynh, N. Jennings, and N. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," Autonomous Agents and Multi-Agent Systems, vol. 13, pp. 119–154, 2006.

[8] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," International Journal of Computational Intelligence Theory and Practice (IJCITP), vol. 5, no. 1, 2010.

[9] J. Zhang and R. Cohen, "Trusting advice from other buyers in emarketplaces the problem of unfair ratings," in Proceedings of the Eighth International Conference on Electronic Commerce, 2006.

[10] Xiaofeng Chen, Jin Li, Willy Susilo, Efficient Fair Conditional Payments for Outsourcing Computations, IEEE Transactions on Information Forensics and Security, 7(6), pp 1687-1694, 2012.

[11] Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang, Wenjing Lou, New Algorithms for Secure Outsourcing of Modular Exponentiations, ESORICS 2012, LNCS 7459, 541–556, Springer-Verlag, 2012.

[12] K. Regan, P. Poupart, and R. Cohen, "Bayesian reputation modeling in e-marketplaces sensitive to subjectivity, deception and change," in Proceedings of the Conference on Artificial Intelligence (AAAI), 2006.

[13] S. Eichler, C. Schroth, and J. Eberspacher, "Car-to-car communication."

[14] J.-H. Cho and A. Swami. Towards trust-based cognitive networks: A survey of trust management for mobile ad hoc networks. In Proceedings of the 14th International Command and Control Research and Technology Symposium, Washington, DC, 2009.

[15] T. Elbatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in Proceedings of VANET, 2006.

[16] Jie Zhang. A Survey on Trust Management for VANETs. 2011 IEEE 105-112.

[17] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust-based message propagation and evaluation framework in vanets," in Proceedings of the Int. Conf. on Information Technology Convergence and services, 2010.