PROCEEDINGS OF SCIENCE

A Real-time Reputation Evaluation Model for Stimulating in MANETs

Yi Cao[1]

Military Representative Office of General Military Equipment Development Department Shijiazhuang Shijiazhuang,050081, China

E-mail: `echo_lzjf @163.com`

Yonghua Huo

The 54th Research Institute of CETC
Shijiazhuang, 050081,China

E-mail: `tsdhyh2005 @ 163.com`

Yingjun Shang

The 54th Research Institute of CETC
Shijiazhuang,050081,China

E-mail: `wjtougao2014@163.com`

Xiaoyu Jin

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing,100876,China

E-mail: `jinxiaoyu@bupt.edu.cn`

With changes in network topology and wireless conflicts, the evidence of trust sampling space may be incomplete or unreliable, which will thus affect the trust evaluation validity. In consideration of inaccurate evaluation in the traditional reputation management mechanism and complexity of the malicious nodes, the Dempster-Shafer (D-S) evidence theory is used to establish the trust evaluation model that can deal with both trust randomicity and subjective uncertainty without prior distribution in evaluation. It also has the recommendation trust filtering mechanism which can monitor the node's behavior at real time, detect and isolate malicious node in time. Theoretical analysis and simulation results show that the proposed model can provide an effective method for trust uncertainty expression and processing, and can effectively resist the attack and reduce the impact of malicious nodes. All in all, our proposed model can promote the detection accuracy ratio and enhance the packets' forwarding services.

CENet2017
22-23 July 2017
Shanghai, China

[1] The work presented in this paper was supported by NSFC(61401033), National Science and Technology Pillar Program Project (2015BAI11B01).

1.Introduction

In the mobile Ad-hoc networks (MANETs), some malicious nodes influence the network function of packet forwarding service. While some selfish nodes always maintain their batteries and feel relunctant to provide extra services for others. Such uncooperative behaviors have a strong impact on packet delivery. With changes in network topology and wireless conflicts, and unsafe network environments in the Ad-hoc networks, it's necessary and important to build a trust evaluation model to monitor the nodes' routing behaviors, and thus improve the network services and capabilities at real time.

The reputation management system can detect and punish the selfish nodes, and encourage the network cooperation. We propose a reputation evaluation model based on D-S evidence fusion in the Ad-hoc networks (RDA). The novel contributions in this paper are shown as follows: (1) we calculate the *Direct Trust* according to the accumulative the direct trust vector during a fixed time interval. The correlation coefficient is introduced to calculate the similarity of two direct trust vectors. (2) A *Recommend Trust Composition process* is proposed based on the improved Dempster-Shafer (D-S) evidence theory. We calculate the basic confidence level and relative importance according to the similar degree of two evidences, and then improve a new fusion rule for reputation evidences.

The rest paper is organized as follows. Section 2 introduces some related works. Section 3 proposes our algorithm and Section 4 simulates the performances of our model and traditional algorithms, and then carries out the result analysis. Section 5 makes conclusion.

2.Related Works

The trust or reputation mechanisms have been widely studied in business Ad-hoc networks or vehicle environments. The reputation management systems detect the malicious nodes in time and thus motivate others to carry out cooperation. As vehicles are deployed autonomously at random, the trust relationships should be established through received messages. Work [1] proposes a privacy-preserving model in the VANETs to protect security by providing accurate reputation-based trust scores. In order to identify the safe message sender, it uses the group signatures to make users anonymous within the same group and identify accountable for the group managers. M Raya et al represent the trust level for entities in data-centric networks. Specially, it takes an example in VANETs[2]. The trust calculation is inferred after it's computed on personal data items. A vehicle is endowed a public or private key pair by a credible CA. The signed message with the private key is provided with authentication services by other nodes that have the sender's public key .

CORE scheme promotes nodes cooperatively in a distributed environment by using collaborative monitoring technique [3]. The entity is responsible for acquiring other entities' behaviors and evaluating their reputations. But the scheme hasn't been directly applied to VANETs because the link between two vehicles is short lived. The reputation information are updated fleetly. And the obsolete reputations cannot realize the accurate trust evaluation.

FIST is a finite-time reputation system for routing forwarding cooperation in the Ad-hoc networks [4]. It aims at resolving problems of lacking rigorous analysis or unreality under existing reputation models. Firstly, it uses perceived probability assumption (PPA) for detecting the neighbors' communications threat to interfere (TTI) and reach subgame perfect Nash

Equilibrium (SPNE). Based on the condition of perceived actions being not seen by both of nodes, the paper proposed FITS-I scheme to perceive forwarding probability.

The reputation evaluation and the reaction system should be homogeneously across time and space. The node behaviors sometimes are driven by changes in the dynamic network environment, therefore, a time-slotted approach can accurately capture the variation of node behaviors. In order to distinguish cooperation and misbehaviors, Work [5] established the detection function to utilize the sequential probability ratio test (SPRT). Except for stimulating the routing forwarding services of selfish nodes, the reputation was also applied to the security routing attacks (e.g., black-hole and gray-hole attacks) in the wireless mesh network [6]. A routing blackhole is a compromised node which can attract traffic for the sake of dropping packets. The grayhole means drop packets selectively. Malicious nodes are not only collude with each other but sponsor the slander attacks to camouflage behaviors and provide fake recommended trust. In the P2P reputation system [7], the local reputation levels are collected and integrated into the global reputation. DHT trust overlay network model stores reputation information to distribute reputation by means of distributed hash table. It avoids the damage of fake reputation information.

3.Reputation Evaluation Model

The trust value depends on the source node's prediction that other nodes supply satisfying network services. The source node evaluates the target nodes' trust values according to their behaviors and the recommendations of other nodes. The former trust relationship is a direct trust and the latter is indirect or recommendation trust. e.g., When Node *A* evaluates the credibility of node *B* in Ad-hoc networks, two important factors need to be considered: one is the direct trust from *A* to *B Trust(D)*, and the other is the recommendation trust from other nodes to *B Trust(I).* At last, Dempster-Shafer evidence theory is used to combine the direct trust and recommend trust, and thus construct the comprehensive trust.

3.1 Direct Trust

Define the direct trust vector on time t_n :

$$D_n=(\alpha_n,\beta_n,\gamma_n) \tag{3.1}$$

Where α_n is the rate of being successful forwarding packets, β_n is the rate of refusal forwarding packets and γ_n is the rate of uncertainty.

The direct trust vector between time t_n and t_{n+1} is defined as:

$$D_{n+1}'=(\alpha_{n+1}',\beta_{n+1}',\gamma_{n+1}') \tag{3.2}$$

$t_{n+1}=t_n+\Delta t$, Δt is a fixed time interval, and D'_{n+1} is the statistics result of forwarding packets during Δt .

Update the direct trust vector after Δt , at t_n and the direct trust vector from t_n to t_{n+1} . The symbol D_{n+1} that denotes the vector is defined as:

$$D_{n+1}=(1-w)\times D_n+w\times D'_{n+1}=(\alpha_{n+1},\beta_{n+1},\gamma_{n+1}) \tag{3.3}$$

w is the weighting coefficient.

In Formula (3.3), D_n is the history direct trust vector, D'_{n+1} is the statistics result in the latest Δt . D_{n+1} considers the history direct trust and recent performance.

The weight *w* in Formula (3.3) is calculated as follows.

We first introduce the correlation coefficient f to calculate the similarity of two vectors. The value ranges of the correlation coefficient are:

$$0 \leq f = sim(D_n, D'_{n+1}) = \frac{\alpha_n \alpha'_{n+1} + \beta_n \beta'_{n+1} + \gamma_n \gamma'_{n+1}}{(\alpha_n^2 + \beta_n^2 + \gamma_n^2)^{1/2} \times (\alpha'^2_{n+1} + \beta'^2_{n+1} + \gamma'^2_{n+1})^{1/2}} \leq 1 \tag{3.4}$$

$$w = \begin{cases} 0.6 + (0.6 - f)^2, f < 0.6\ and\ (\alpha'_{n+1} - \alpha_n) < (\beta'_{n+1} - \beta_n) \\ f^2, \quad f < 0.6\ and\ (\alpha'_{n+1} - \alpha_n) \geq (\beta'_{n+1} - \beta_n) \\ 0.6, \quad f \geq 0.6 \end{cases} \tag{3.5}$$

As indicated by Formulas (3.4) and (3.5), we know that the more similar the two vectors are, the larger the correlation coefficients f will be. When f <0.6, it signifies the changes between D_n and D'_{n+1} are large. When $(\alpha'_{n+1} - \alpha_n) < (\beta'_{n+1} - \beta_n)$, it means the current services are worse than the services in the past, so let the value of *w* be large to strengthen the impact of the current bad services. A larger *w* means D'_{n+1} carries a bigger weight, thus the malicious nodes that provide good services in the past, but provide bad services recently can be detected quickly. When $(\alpha'_{n+1} - \alpha_n) \geq (\beta'_{n+1} - \beta_n)$, the *w* is f^2 because the trust vector of the current good services performs dissimilarly to the trust vector of the bad services in the past time. In this sense, it can only gain a small weight. As the poor records cannot be changed rapidly, the malicious nodes are forced to provide better routing forwarding services to other nodes for quite a while.

If the node performs maliciously, slanderously or selfishly, then the weight of the current bad services will be expanded; besides, the measurements can also weaken the influence of malicious nodes.

3.2 Baased D-S Theory Recommendation Trust Composition Rule

The Dempster-Shafer evidence theory provides the representation of both imprecision and uncertainty by using the probabilities of a collection of hypotheses. Define θ be the frame of discernment. $\theta = \{\theta_1, \theta_2, ... \theta_N\}$ is the set corresponding to *N* objects. Then 2^{Θ} denotes the power set of θ . A basic probability assignment *m* defined on 2^{Θ} is denoted as:

$$m: 2^{\Theta} \rightarrow [0,1] \tag{3.6}$$

$$\sum_{A \in 2^{\Theta}} m(A) = 1, \qquad m(\phi) = 0 \tag{3.7}$$

Firstly, we define the recommended trust vector from node *i's* neighbor node *k* to the node *j*, where *i* is the source node and *j* is the target node.

$$m_{n_k, j} = (m_{k,j}(\{T\}), \quad m_{k,j}(\{{}^{\sim}T\}), m_{k,j}(\{T, {}^{\sim}T\})) \tag{3.8}$$

Suppose that $m_{n_k, j}$ is the basic probability assignments over the frame of discernment W from neighbor node *k* to target node *j*. Intuitively, $m_{k,j}(A_i)$ describes the extent to which the evidence supports A_i, where $A_i \subseteq 2^W$, and clearly the frame of discernment in our evidence model is $W = \{T, {}^{\sim}T\}$. Before the improvement of D-S, we introduce several definitions.

Definition 1. The information capacity of an evidence $m_{n_k, j}$ is defined as:

$$e(m_{n_k, j}) = \sum_{i=1}^{l} \frac{m_{k,j}(A_i)}{\|A_i\|} \tag{3.9}$$

Where A_i is the focal element, $A_i \subseteq 2^W$ and $A_i \neq \emptyset$. And then $W=\{T, {}^{\sim}T\}$ is the frame of discernment in our reputation evidence model. Parameter l is the number of focal elements, and $\|A_i\|$ is the number of components in the focal element A_i , $\sum_{i=1}^{l} m_{k,j}(A_i)=1$. In our evidence fusion model, $A_i=\{\{T\},\{{}^{\sim}T\},\{T, {}^{\sim}T\}\}$ and $l=3$.

We transfer the basic probability assignments by multiplying the information capacity.

$$\begin{cases} m_{k,j}'(A_i)=m_{k,j}(A_i)e(m_{n_k,j}) \\ m_{k,j}'(\theta)=m_{k,j}(\theta)e(m_{n_k,j})+(1-e(m_{n_k,j})) \\ m_{k,j}'(\emptyset)=0 \end{cases} \tag{3.10}$$

Definition 2. The distance between two evidences $m_{n_k,j}$ and $m_{n_m,j}$ is:

$$d(m_{n_k,j}, m_{n_m,j})=\sqrt{\frac{1}{2}(m_{n_k,j}-m_{n_m,j})^T(m_{n_k,j}-m_{n_m,j})} \tag{3.11}$$

The distance between two evidences is used to measure the similarity of them. For excemple: $m_{n_k,j}$ =(0.3,0.6,0.1), $m_{n_m,j}$ =(0.2,0.7,0.1), the distance between the evidences is 0.1.

Where $m_{n_k,j}=(m_{k,j}(\{T\}), m_{k,j}(\{{}^{\sim}T\}), m_{k,j}(\{T, {}^{\sim}T\}))$, and $0 \leq d(m_{n_k,j}, m_{n_m,j}) \leq 1$.

Definition 3. The similar degree of two evidences $m_{n_k,j}$ and $m_{n_m,j}$ is:

$$s(m_{n_k,j}, m_{n_m,j})=1-d(m_{n_k,j}, m_{n_m,j}) \tag{3.12}$$

As we can see, the greater similar degree of $m_{n_k,j}$ and $m_{n_m,j}$, the more similar analysis the two evidences describe. If we have one evidence which is similar to all of others, then we believe that this evidence is important. Supposing that node *i* has *n* neighbor nodes, the corresponding basic probability assignments are $\{m_{n_1,j}, m_{n_2,j}, \ldots, m_{n_n,j}\}$.

Definition 4. The *basic confidence* β_k of $m_{n_k,j}, (k=1,2,\ldots n)$ is:

$$\beta_k=\sum_{m=1}^{n} s(m_{n_k,j}, m_{n_m,j}) \tag{3.13}$$

The *relative importance* ψ_k of $m_{n_k,j}$ to the evidence that has the greatest *basic confidence*:

$$\psi_k=\beta_k / max_{1 \leq m \leq n} \beta_m \tag{3.14}$$

Finally, we have the new fusion rule:

$$\begin{cases} m(A)=\sum_{\cap A_i=A} \prod_{1 \leq k \leq n, 1 \leq i \leq 3} m_{k,j}'(A_i)+k'q'(A) \\ m(\emptyset)=0 \end{cases} \tag{3.15}$$

Where $m_{k,j}'(A_i)$ is calculated according to Formula (3.9), $k'=\sum_{\cap A_i=\emptyset} \prod_{1 \leq k \leq n, 1 \leq i \leq 3} m_{k,j}'(A_i)$, and $q'(A)=\sum_{k=1}^{n} \psi_k m_{k,j}'(A)$.

The fusion rule to get the final recommend trust. *m(A)* is the final probability assignment for A_i. Formula(3.15) is the evidence combination rule, *q'(A)* consider the relative importance of every probability assignment for *A*. So a malicious node that provides conflicting recommend trust will have less *basic confidence,* thus has less influence on the final composition.

4. Simulation Results Analysis

To analyze the performances of the Reputation evaluation based on D-S evidence fusion models in the Ad-hoc networks (RDA), we conducted simulations with D-S based on Watchdog and the local trust-based resource allocation (LTRA) [8]. The Watchdog is a secure scheme which uses overheard messages to police their downstream neighbors locally by enabling nodes to detect malicious behaviors probabilistically. LTRA proposed a technique of resource and reputation monitoring for "trustworthiness evaluation" by using self-assessment based scheme. Assume that there are 120 nodes in which the total number of malicious nodes is 40. The malicious nodes include the selfish nodes, the slander nodes and the collusion nodes. The malicious behaviors don't occur throughout the process of simulation instead of the probabilities of occurrence fluctuate within [0.2, 0.5].

In Fig. 1, we verified the routing forwarding rates with different numbers of detection iteration. The simulation results have demonstrated the execution of routing forwarding services throughout the detection process. Here the occurrence probabilities of selfish nodes, slanderous nodes and collusive nodes were 0.2, 0.2 and 0.3 respectively. We tested 200 detection iterations for all of nodes in the Ad-hoc networks. We can see that the ratios among three detection algorithms had a sharply downtrend before 60-80 iterations, and rose slowly in the remainder iterations. Here the average ratio of RDA had 3.49% and 7.07% higher than that of LTRA and Watchdog. In comparison with the other two detection algorithms, RDA featured a higher detection accuracy on account of improvement for fusion rule of reputation evidences.

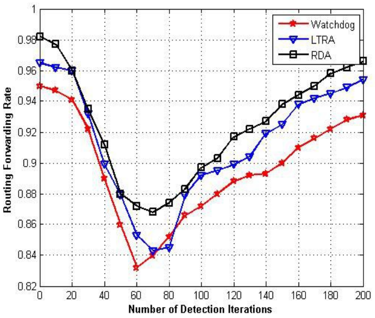

Figure 1: Routing Forwarding Rates with Different Number of Iterations

According to Fig.1, the detection accuracy rates of selfish nodes with different iterations have obviously distinction. We simulated the indicators at the 60th iteration and results analysis are represented in Fig. 2.

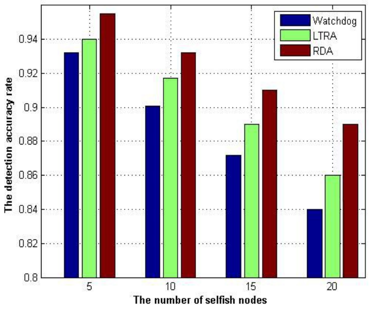

Figure 2: Detection Accuracy Rates with Different Selfish Nodes

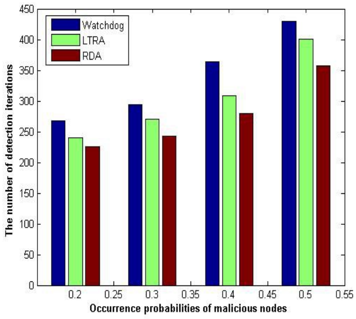

Figure 3: The Number of Iterations with Different Occurrence Probabilities

When the number of iteration is within [60, 70], RDA has the lowest routing forwarding rate according to results in Figure 1. Although the detection accuracy rate is less than 0.9 when the number of selfish nodes reach the maximum, it is bigger than that of Watchdog and LTRA depicted in the Fig. 2. The average detection ratio of RDA is 3.21% and 3.78% higher than that of LTRA and Watchdog.

Fig. 3 represents the number of detection iterations with different occurrence probabilities when searching out all of malicious nodes. As the occurrence probabilities continually rise from 0.2 to 0.5, the number of detection iterations also grow accordingly. RDA has 14 and 42 iterations respectively, which are less than that of LTRA and Watchdog when all of occurrence probabilities of malicious nodes (including selfish, slanderous and collusive nodes) are 0.2. While the value increases to 44 and 72 iterations when all of occurrence probabilities are 0.5. It demonstrates that our algorithm features superior performances for searching all of malicious nodes.

5.Conclusion

The paper proposes a Reputation evaluation based on D-S evidence fusion models in the Ad-hoc networks (RDA). The stimulation mechanism calculates and integrates the direct trust and recommended trust scores. Therefore, the recommend trusts provided by malicious nodes will not be used in the recommended trust composition process. The RDA model can deal with uncertainty in the process of reputation evidence evaluation and detection of malicious nodes.

References

[1] A. Tajeddine, A. Kayssi, A. Chehab. *A Privacy-Preserving Trust Model for VANETs*. International Conference on Computer and Information Technology, 2010.

[2] M Raya, P. Papadimitrators, V.Gligor, J.P.Hubaux. *On data-centric trust establishment in ephemeral Ad-hoc networks*. IEEE Conference on Computer Communications (INFOCOM). 2008. pp. 1238-1246.

[3] P. Michiardi and R. *Molva Core: A collaborative reputation mechanism to enforce node cooperation in mobile Ad-hoc networks*. Communications and Multimedia Security Conference (CMS). 2002.pp. 107-121.

[4] C. Tingting, W. Fan, Z. Sheng. *FITS: A Finite-Time Reputation System for Cooperation in Wireless Ad-hoc Networks.* In: IEEE Transactions on Computers, vol. 60(7), 2011, pp.1045-1056.

[5] M.T. Refaei, L.A. DaSilva, M. Eltoweissy, T. Nadeem. *Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad-hoc Networks*. In: IEEE Transactions on Computers. 2010. 59(5):707-719.

[6] F. Oliviero, S.P. Romano. *A Reputation-Based Metric for Secure Routing in Wireless Mesh Networks.* IEEE Global Telecommunications Conference (GLOBECOM). 2008. pp. 1-5.

[7] L. Yaqiong, X. Weilian, L. Keqiu, C. Zhongxian, M. Geyong, Q. Wenyu. *DHTurst: a robust and distributed reputation system for trusted peer-to-peer networks.* IEEE Global Telecommunications Conference (GLOBECOM). 2010. pp.1-6.

[8] Varalakshmi, P. ; Judgi, T. ; Hafsa, M.F. *Local trust based resource allocation in cloud.* Fifth International Conference on Advanced Computing (ICoAC). 2013. pp. 591 – 596.