18

Secure Trust-based Cooperative Communications in Wireless Multi-hop Networks

Kun Wang, Meng Wu and Subin Shen
Institute of IOT, Nanjing University of Posts and Telecommunications, Nanjing, China

1. Introduction

The word cooperate derives from the Latin words co-and operate (to work), thus it connotes the idea of "working together". Cooperation is the strategy of a group of entities working together to achieve a common or individual goal. The main idea behind cooperation is that each cooperating entity gains by means of the unified activity. Cooperation can be seen as the action of obtaining some advantage by giving, sharing or allowing something. Cooperation is extensively applied by human beings and animals, and we would like here to map different cooperation strategies into wireless communication systems. While the term cooperation can be used to describe any relationship where all participants contribute, we tend to use it here to describe the more restrictive case in which all participants gain. If we use it in the broader sense of simply working together, it will be apparent from the context or explicitly stated. This restricted definition of cooperation contrasts with altruism, a behaviour where one of the participants does not gain from the interaction to support others (Frank & Marcos, 2006).

Cooperation has become an academic subject of intensive study in the social and biological sciences, as well as in mathematics and artificial intelligence. The most fundamental finding is that even egoists can support cooperation if necessary. In the field of information systems, some notable illustrations of this principle have recently emerged. One example is the success of open source in which thousands of people have cooperatively created a system, such as Linux. Another example is the success of eBay, which is based on a feedback system by verifying the accumulated reputations through cooperating with others in the past, making strangers mutually trust.

Recently, Wireless multi-hop networks provide yet another realm in which cooperation among large numbers of egoists can be attained, provided that the right institutional structure can designed and implemented. Wireless communications is a rapidly emerging area of technology. Its success will depend in large measure on whether self-interested individuals can be provided a structure in which they are proper incentives to act in a cooperative mode. Cooperative techniques can be employed across different layers of a communication system and across different communication networks. The foremost premise of cooperative techniques is through cooperation, all participants engaged in cooperative communication may obtain some benefits.

Source: Communications and Networking, Book edited by: Jun Peng,
ISBN 978-953-307-114-5, pp. 434, September 2010, Sciyo, Croatia, downloaded from SCIYO.COM

An analogy between cooperation in natural and human sciences with the world of wireless communications can sometimes be established, though it is not our aim here to identify all such possibilities. It is interesting to note that in nature cooperation can take place at a small scale (i.e., few entities collaborate) or large scale (i.e., massive collaboration). The latter includes cooperation between the members of large groups up to the society itself. A similar classification holds in the wireless domain. A few nodes (e.g., terminals, base stations) can cooperate to achieve certain goals. The foreseen wireless knowledge society is expected to be a highly connected (global) network where virtually any entity (man or machine) can be wirelessly connected with each other. Cooperation in such a hyper–connected world will play a key role in shaping the technical and human perspectives of communication.

In wireless network field, Ad Hoc networking has been an attractive research community in recent years. A mobile Ad Hoc network is a group of nodes without requiring centralized administration or fixed network infrastructure, in which nodes can communicate with other nodes out of their direct transmission ranges through cooperatively forwarding packets for each other. In Ad Hoc networks, all networking functions must be performed by the nodes themselves. Each node acts not only as a terminal but also a router. Due to lack of routing infrastructure, they have to cooperate to communicate, discovering and maintain the routes to other nodes, and to forward packets to their neighbours. Cooperation at the network layer means routing (i.e., finding a path for a packet) and forwarding (i.e., relaying packets for others). While nodes are rational, their actions are strictly determined by their own interests, and each node is associated with a minimum lifetime constraint. Therefore, misbehavior exists, and it also occurs to multi-hop cellular networks. Misbehavior means deviation from regular routing and forwarding. It arises for several reasons; unintentionally when a node is faulty for the linking error or the battery exhausting. Intentional misbehavior can aim at an advantage for the misbehaving node or just constitute vandalism, such as enabling a malicious node to mount an attack or a selfish node to save energy. Malicious nodes are nodes that join the network with the intent of harming it by causing network partitions, denial of service (DoS), etc. The aim of malicious node is to maximize the damage they can cause to the network, while selfish nodes are nodes that utilize services provided by others but do not reciprocate to preserve their resources. These nodes do not have harmful intentions toward the network, though their Denial of Service actions may adversely affect the performance of the network, and turn the wireless network into an unpractical multi-hop network. The aim of selfish nodes is to maximize the benefits they can get from the network. In game-theoretic terms, cooperation in mobile ad hoc networks poses a dilemma. To save battery, bandwidth, and processing power, selfish nodes will refuse to forward packets for others If this dominant strategy is adopted, however, the outcome isn't a functional network when multi-hop routes are needed, and all nodes are worse off. Therefore, incentive cooperation will inevitably be the key issue in cooperative communications.

In the social network, trust relationship is the essence of the interpersonal relationship. The trust among individuals depends on the recommendation of others; at the meanwhile, the credit of recommenders also determines the credit of the one they recommend. Actually, this kind of interdependent relationship composes an alleged web of trust (Caronni, 2000). In such a trust network, the trust of any individual is not absolutely reliable, but can be used as other individual's reference for their interactions. The individuals in web of trust and interpersonal network have great similarities, which are reflected in:

1. In the network, individuals in the interaction may leave sporadic "credit" information;
2. Individuals have full right to choose interactive objects;
3. Individuals have the obligation to provide recommended information to other individuals in the network.

Thus, using some conclusions from the sociological research for reference to apply all these notions to the problem of reliable packet delivery in MANETs becomes possible. However, Trust establishment is an important and challenging issue in the security of Ad Hoc networks. The lack of infrastructure in MANET makes it difficult to ensure the reliability of packet delivery over multi-hop routes in the presence of malicious nodes acting as intermediate hops.

Before we can compare different trust evaluation methods or discuss trust models for Ad Hoc networks, a fundamental question needs to be answered first. What is the physical meaning of trust in Ad Hoc networks? The answer to this question is the critical link between observations (trust evidence) and the metrics that evaluate trustworthiness. In Ad Hoc networks, trust relationship can be established in two ways. The first way is through direct observations of other nodes' behaviour, such as dropping packets etc. The second way is through recommendations from other nodes. Without clarifying the meaning of trust, trustworthiness cannot be accurately determined from observations, and the calculation/policies/rules that govern trust propagation cannot be justified.

Another security issues of distributed networks such as P2P, Ad hoc and wireless sensor networks have also drawn much attention. Cooperation between nodes in distributed networks takes significant risks, for a good node in an open network environment may suffer malicious attacks while obtaining reliable resources. Such attack can lead to the decline in the availability of network application.

Distributed trust management can effectively improve the security of distributed network. A reputation model is constructed based on the historical transactions of nodes. When a node determines to cooperate with another node, the trust value of the node should be taken into consideration first (Paola & Tamburo, 2008).

Nodes in reputation model share the result of transactions. A node considers evaluations of another node from transaction history when determining to make transactions. These evaluations may be incorrect sometimes so the research on the relationship between an evaluating node and a node being evaluated is worth exploring. It can help the reputation model decrease malicious evaluation, collect more subjective evaluations and eventually calculate the global trust value.

Current reputation models often adopt single trust, which fails to fully describe node behavior. Also, reputation model mainly researches on methods of trust measurement and analyzes the effectiveness of mathematical model with global trust value. However, the issue whether the established mathematical model is vulnerable or not is rarely discussed.

In this way, we introduce the trust model of social networks into reputation model in multi-hop networks, construct a global dual trust value for each node dramatically based on the nodes historical transactions, present a robust, cooperative trust establishment scheme in the model that enables a given node to identify other nodes in terms of how "trustworthy" they are with respect to reliable packet delivery and discuss how this model manages to resist different attacks. The proposed scheme is cooperative in that nodes exchange information in the process of computing trust metrics with respect to other nodes. On the other hand, the scheme is robust in the presence of malicious nodes that propagate different attacks.

The rest of the chapter is organized as follows: section 2 briefly introduces the related work with the writer's research and point of view, and then proposes a reputation-based trust management model in multi-hop network in section 3. Section 4 introduces an updating algorithm of trust value, so that the reputation model itself can effectively resist different attacks. Simulation results are presented in section 5 to prove the validity of the model. Section 6 discusses security issues in trust model in detail, and compares some related trust model with our research. Finally, section 7 concludes the chapter and points out some aspects of future research.

2. State-of-the-art

Cooperative techniques in wireless networks can be classified as follows (Frank & Marcos, 2006), shown in Fig. 1:

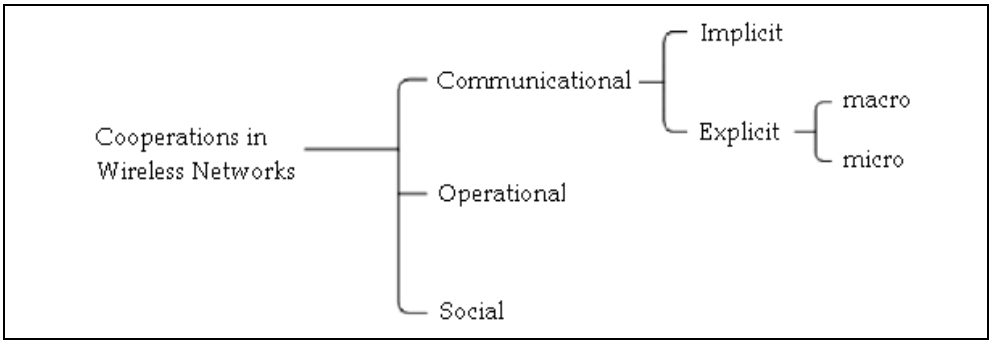


Fig. 1. A practical classification of cooperation in wireless networks

1. Communicational cooperation, which can further categorize cooperation as either Implicit, or Explicit Macro, or Explicit Micro (Functional) Cooperation. Examples of implicit cooperation are communication protocols such as TCP and ALOHA. In such protocols, participants share a common resource based on fair sharing of that resource but without the establishment of any particular framework for cooperation. In contrast, explicit macro cooperation is characterized by a specified framework and established by design. Cooperative entities that fall in this category are wireless terminals and routers, which may cooperate, for example, by employing relaying techniques that extend the range of communication for users beyond their immediate coverage area. Such cooperation potentially provides mutual benefits to all users. Explicit micro or functional cooperation is also characterized by a specific framework that is established by design. However, the cooperation involves functional parts or components of various entities, such as antennas in wireless terminals, processing units in mobile computing devices, and batteries in mobile devices. Explicit micro cooperation provides the potential for building low complexity wireless terminals with low battery consumption.
2. Operational cooperation, referring to the interaction and negotiating procedures between entities required to establish and maintain communication between different networks. The main target here is to ensure end-to-end connectivity, where the main players are (different) terminals operating in different networks. Network architecture and setup procedure are the main content of this category.

3. Social cooperation, pointing out the dynamic process of establishing and maintaining a network of collaborative nodes (e.g., wireless terminals). The process of node engagement is important as each node needs to decide on its participation in this ad hoc communication, having each decision an individual and collective impact on performance. Unlike the previous categories, in this arrangement each node is in a key position as he or she ultimately decides whether to cooperate or not. Appealing incentives need be offered to the nodes in order to encourage them to cooperate. The incentives in social cooperation are our research point.

In Ad Hoc networks, the incentive schemes can be roughly classified into reputation-based system and payment-based system. Here the latter is beyond the range of our study. In reputation-based systems, nodes observe the behaviour of other nodes and take measures, rewarding cooperative behaviours or punishing uncooperative behaviours. The typical models of this scheme include CONFIDANT (Buchegger & Le Boudec, 2002), CORE (Michiardi & Molva, 2002) and SORI (He & Wu, 2004).

CORE provides three different types of trust: subjective trust, indirect trust and functional trust. The weighted values of these three trusts are then used to determine whether to cooperate or not. CORE system allows nodes in MANET gradually to isolate malicious nodes. When the reputation assigned to a neighbour node decreases below a predefined threshold, the service provided for the misbehaving nodes will be interrupted. However, CORE system doesn't take the forged situation of indirect trust into consideration, for nodes could raise indirect trust by mutual cooperative cheating.

The goal of SORI system is to resist DoS attacks, using a similar watchdog-like mechanism to monitor. The information that reputation system maintains is the ratio of forwarded packets over sent packets. However, SORI system needs to authenticate the evaluation of reputation based on Hash function, which may naturally increase the overload of the system.

CONFIDANT is a reputation system containing monitoring, trust evaluation and trust reestablishment. This system only adopts periodic decay of trust to avoid non-cooperative behaviors without providing redemption mechanism for nodes. Yet the redemption mechanism is very important to isolated nodes, because the malicious actions of these nodes may be due to other non-malicious factors (battery energy exhausting, linking error, etc.).

Currently, the reputation models can be roughly categorized as follows:

1. Reputation models based on Public Key Infrastructure (PKI). Millan et al. adopt the approach of Cross-layer Authentication (Millan, Perez, et al., 2010), the author described the design, implementation and performance evaluation of Cross-layer. The legality of these nodes can be guaranteed by the certifications from Certificate Authority (CA). Omar et al. introduces a distributed PKI certification system based on Trust Map and Threshold Encryption (Omar, Challal, et al., 2009). Node legality is secured by Certificate Chain. However, CA will inevitably cause the problems on expansibility and invalidation of single node.

2. Reputation models based on Markov Chain. Chang et al. adopts Markov Chain to determine the trust value of the single-hop node. The node whose trust value achieves the highest will be set as the central node (Chang, Kuo, 2009). ElSalamouny et al. adopts a sort of potential Markov Chain to indicate the key behaviour of the node, and makes use of the beta probability distribution and exponential decay to evaluate the trust error (ElSalamouny, Krukow, et al., 2009). However, neither of these two reputation models involves node attacks.

3. Reputation models based on Random Probability Model [7-10], such as Power-law Distribution and Bayesian. PeerTrust (Li & Lu, 2004) controls the feedback weighting by comparing the similarity of evaluation of previous co-operator, and separates the service trust and feedback trust. But with the growth of network scale, the statistical analysis of set becomes difficult. In PowerTurst (Zhou & Hwang, 2007), there is no consideration of the malicious, selfish or strategic actions. RSFN (Saurabh, Laura, et al., 2008) adopts Bayesian Model to update the reputation with new transaction evaluation, introduces the updating algorithm between dual evaluation and zone [0,1] evaluation, and uses the algorithm to avoid bad mouthing and boost attacks during the reputation establishment process. Nevertheless, there is no further discussion regarding the effects of other types of attacks.
4. Reputation models based on fuzzy control. Ganeriwal et al. introduce a central reputation model based on a trust value pair(trust/non-trust), and set 'trust', 'non-trust', 'ignore', and 'variance' as the fuzzy controlling parameters (Victor, Cornelis, et al., 2009). However, the author doesn't consider the security issues, and the problem of CA still exists. RFSTrust (Luo, Liu, et al., 2009) is a reputation model based on fuzzy recommendation. Node trust value includes five fuzzy controlling parameters. On the security issue, the author only mentioned the selfish behaviour of nodes, but no other attacks.
5. Reputation models based on direct trust and recommendation trust [13-18]. Peng et al. adopted abnormal trust series to detect the malicious and fake recommendation, and to defend against collusion attacks (Peng, He, et al., 2008). Liu et al. proposed a two dimensional reputation model based on time and context to resist collusion attack (Liu & Issarny, 2004). Li et al. use the distance weighting-based reputation model, with Distributed Hash Table (DHT) to manage the node trust value (Li & Wang, 2009). The node trust value is evaluated according to the distance between the nodes. Sun et al. discusses the multi-defence structure reputation model based on direct and recommendation trust (Sun, Liu, et al., 2008). However, the collected trust information is not comprehensive, hence leading to the inaccuracy of trust evaluation. TrustMe (Aameek & Liu, 2003) adopt the anonymity to encourage the nodes to provide the honest information without worrying about vengeance. Two IDs are distributed to each node. One is used for transaction, and the other one is used for reputation evaluation. In addition, the model uses the central login server to distribute the unique ID to reduce the cheating and newcomer attacks. However, because reputation update and searching processes happen among nodes, dishonest evaluation of node transaction can not be prevented even though transaction certificate is required for transaction evaluation, Yu et al. introduce a dual evaluation model based on feedback trust and service trust (Jin, Gu, et al., 2007). It compares these two values to resist the malicious feedback. However, little information has been done on how to determine the consistency of these two values.
Besides, many typical reputation models have failed to consider the security issue or merely considered one or several kinds of attacks without fully analyzing the malicious, selfish and strategic behaviors. For instance, EigenTrust (Sepandar, Mario, et al., 2003) introduces a fully distributed reputation model without central login server. Nevertheless, the node ID is easy to be changed. As a result, the network is vulnerable to newcomer attack. Based on wireless sensor networks, RDAT (Ozdemir, 2008) uses different models separately to discuss the trust value of perception, routing and collection to find the malicious behaviors of each phase. TOMS (Boukerche & Ren, 2008) updates trust value based on a nonlinear algorithm, and selects trust router to exchange information in order to reduce the access of malicious

nodes to some extent. Ding et al. introduce a dynamic trust management model (Ding, Yu, et al., 2008). In a P2P file sharing application, when trust value is lower than a set threshold, a message for warning nodes malicious behaviors will be sent out to other nodes so as to control the transmission of malicious files. However, this method will be taken advantage of by some malicious nodes to defame trusted nodes.

Based on the related work above, current reputation model is mainly single trust, and doesn't consider the capability of preventing attacks. Therefore, this article introduces a trust management model based on global reputation. Meanwhile, we use the updating algorithms of trust value to comprehensively analyze the resistant mechanism of this model for different attacks.

3. Reputation-based trust management model

3.1 Model outline

In multi-hop networks, nodes provide data and service for each other, and execute distributed trust management. If logic networks are distributed, non-structural and self-organized, each node in the networks will independently determine which node it will interact with. One node can receive an evaluation after providing service to the other. Therefore, nodes reputation can be considered as the integration of evaluations from others. As a service request node, it needs reputation information from service provider. Afterwards, it selects an appropriate service provider to interact with its own strategy. As a service provider, each node expects its own trust value to be as high as possible. In this way, it can have many "customers" and benefit from the model incentive mechanism as well. However, honest nodes achieve high reputation by offering honest service, while malicious nodes gain reputation by tampering or decreasing other nodes trust value so that they obtain more chances in order to be a service provider. Undoubtedly, a good service provider only responds to the node with high trust value in terms of its own strategy. As a result, a node can get better service when it works as a request node and has high trust value.

Distributed trust management model is local recommendation-based or reputation-based. In this chapter, we focus on the latter one, i.e., when selecting a service provider, each node calculates the trust value of each response mode (the trust value here is the integration of local trust and global trust). Then a node selects provider with high trust value with reference to its own strategy. In this case, malicious behaviors can be controlled to a certain extent with the increase of networks robustness.

Our aim of trust management model is that an honest node only costs little to prevent malicious behaviors. We analyze and design the model according to nodes honest behaviors, malicious attacks and multi-hop networks environment (Marti & Molina, 2006).

3.2 Model design

Most of current trust management models use dual evaluation or zone [0, 1] for evaluation (Yu, Singl, et al., 2004). Dual evaluation is not subjective, but it enables node to get a high trust value by a few successful transactions, which is vulnerable to outside attacks. So our model herein uses zone [0, 1] for evaluation, which enhances the pluralism of trust value and also ensures the continuity of it. We set nodes initial trust value to be 0.5, and after several transactions, the trust value of honest nodes is close to 1 while that of malicious ones will drop to less than 0.5.

There are some nodes called strategy nodes. They initially behave well and get high trust value after joining in networks. Afterwards, they start to behave maliciously, reducing QoS or providing dishonest feedback. The most common method to fight against these attacks is to implement punishment mechanism to decrease their trust value. However, some strategy nodes only offer dishonest feedback but without reducing their own QoS. If single trust is employed, the trust value of these nodes will decrease sharply and cannot show their service abilities.

In view of the situation above, we set two trust values, for each node in our model. One is service trust value (STV), providing the global trust value of the service; the other is request trust value (RTV), providing the global trust value of the evaluation. Both sides evaluate each other and update STV and RTV after each transaction. This dual trust values strategy is more flexible to fight against the attacks. We here set an example to illustrate the execution process of dual trust values in detail, shown in Fig. 2:

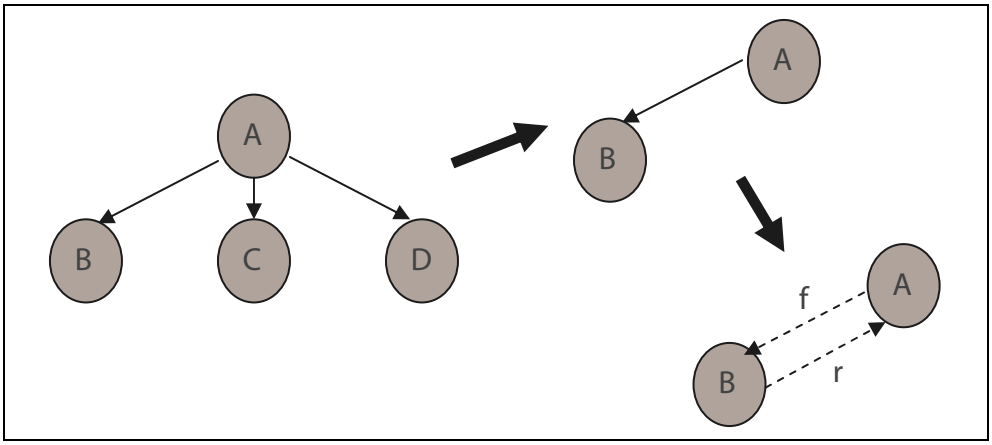


Fig. 2. Execution Process of Dual Trust Values

1. Supposing that node A has sent out a resource request and node B, C, and D have received it. They start to analyze the request and make response according to their own strategies (The analysis here includes evaluating the RTV of node A, checking whether they have such resource, etc.).
2. Node A will select the node with the highest trust value (for instance, here is node B) in terms of the local trust value (LTV: this trust value is STV stored locally, and it exists if transactions happened between them, otherwise it is set default) and the STV of responding node.
3. After selecting node B, node A will give node B an evaluation 'r' based on the transaction and its own strategies (for example, whether it is a malicious node or whether the response contains malicious information) Meanwhile, node B will give a feedback 'f' to node A as well.
4. Based on the feedback node A gives to node B, node A will calculate and update the STV of node B and save it as LTV as well.
5. Meanwhile, according to the feedback node B gives to node A, node B will calculate and update the RTV of node A.

In our model, we do not discuss which node(s) will be responsible for the calculation and storage of STV and RTV, because an agent or a neighbour node can accomplish the tasks (Thomas & Vana, 2006). To simplify the model, we suppose a central server to store and calculate STV and RTV (Zhang & Fang, 2007), while LTV is saved by a node itself.

From the view of social network, if a requester evaluates a service provider, the service provider will also evaluate the feedback of that requester. Due to revengeful psychology, feedback evaluation is normally in accord with service evaluation, that is, I will give you what you give me. Honest nodes provide honest service and feedback, while dishonest nodes provide neither honest service nor honest feedback. We can analyze the effect of mutual evaluation on reputation model by four scenarios as below, shown from Fig. 3 to Fig. 6.

Scenario 1: Service requester is an honest node while service provider is a malicious node. In this case, the mutual evaluation is bad. As a result, both the STV of malicious node and the RTV of honest node decrease. Thereby malicious nodes will have low probability to be selected as provider after some transactions.

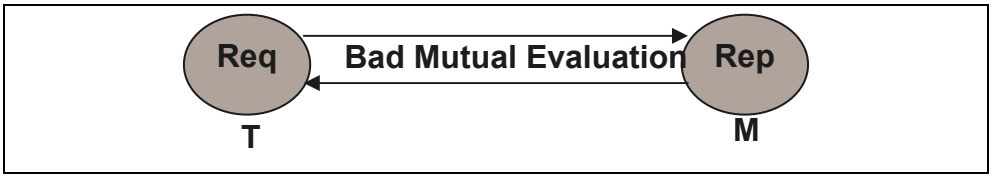


Fig. 3. Scenario 1

Scenario 2: Service requester is a malicious node while service provider is an honest node. In this case, the mutual evaluation is bad. However, service provider in our model only responds to the requester whose trust value is high. Therefore, the possibility of this scenario is very low.

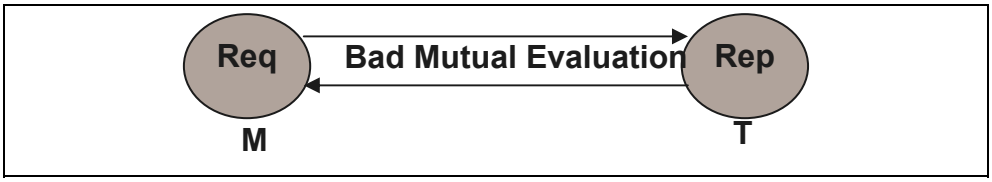


Fig. 4. Scenario 2

Scenario 3: Both service requester and provider are honest nodes. In this case, the mutual evaluation is good. When the malicious node in networks is not large scale, transactions should be in this scenario.

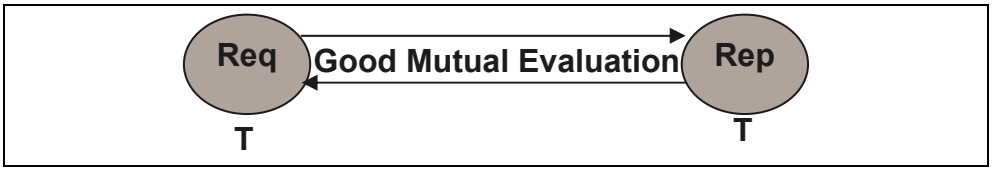


Fig. 5. Scenario 3

Scenario 4: Both service requester and provider are malicious nodes. If both sides are collusion nodes, the mutual evaluation is good. Otherwise, it is bad. The former case should be eliminated.

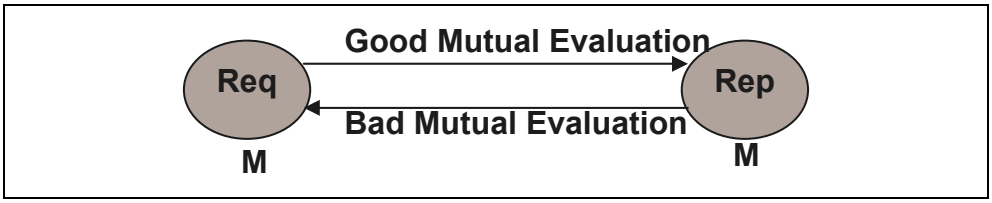


Fig. 6. Scenario 4

Some nodes only provide honest service but not honest feedback or vice verse. The influence of these nodes also includes in the scenarios above, which decreases certain trust value of the node.

Incorrect evaluation in Scenario 1, 2 and 4 will affect the reputation model. Scenario 1 and 2 can cause imputation attacks, and Scenario 4 can lead to collusion attacks. Furthermore, the effect of other attacks on the reputation model should also be considered.

4. Robustness analysis of reputation model

In this section we propose an updating algorithm of trust value to defend against different attacks. Other security problems, such as data transmission, can be resolved by encryption authentication technology. Ma et al. put forward a kind of fragment multipath transmission protocol to defend against man-in-the-middle attack, which protects the integrality of trust information (Ma & Qin, 2007). In this case, we only discuss the malicious behaviors and defending mechanism which is directly related to reputation model.

4.1 Updating algorithms of trust value

Assuming that the information collected from central node is correct and integrated, that is, not tampered or lost. We can use the statistical approach to update node STV.

Node STV updating algorithm: comparing the similarity of STV after transaction with the previous value, and updating it on the basis of original STV. More specifically, updated STV uses self-adaptive algorithm. If original STV reaches 0.5, new evaluation will affect the STV a lot. Otherwise, if STV reaches 0 or 1, the influence will be tender. Moreover, if STV this time is higher than original one, it will increase a little; otherwise, it will decrease a lot, compared with the rising extent. Here we set a mathematic model to illustrate this algorithm.

Definition: Supposing STV is T_n after the (n)th transaction of each node, and evaluation is r after the (n+1)th transaction. In this algorithm, the updating STV is:

$$T_{n+1} = \begin{cases} T_n + (r - T_n) / 2 \times \theta \times \lambda_1 & r \geq T_n \\ T_n + (r - T_n) / 2 \times \theta \times \lambda_2 & r < T_n \end{cases} \quad (1)$$

Where

$$\theta = 1 - (2T_n - 1)^2 \quad (2)$$

Then define

$$\lambda = \lambda_1/\lambda_2 \quad (0<\lambda_1<\lambda_2<1) \tag{3}$$

θ in equation (1) stands for the function of T_n, shown in equation (2). It is used to adjust the weighting between historical STV and current evaluation. When historical STV is close to the original trust value, current evaluation should be emphatically considered. On the contrary, when historical trust value is far away from the original trust value, historical evaluation should be focused on.

In equation (3), λ_1 and λ_2 indicate respectively the increasing and decreasing extent of STV after each successful transaction, while λ shows the ratio of increasing extent to decreasing extent. Generally, decreasing extent is greater than increasing extent, controlled by λ. Furthermore, the algorithm can also be designed as: when the STV decreases to a given threshold even though the later transaction is honest, the increasing extent of STV will still be less than the decreasing one. In this way, the malicious behaviors can be published dramatically.

Since updating algorithms of RTV and STV are the same, there is no further discussion here.

4.2 Attacks and defenses

Strategy node attacks

Generally, strategy nodes achieve high trust value through some small transactions. Afterwards, they execute a big cheat. Repeatedly, they obtain the maximum benefits with minimum cost. Therefore, our reputation model needs to make the rising of trust value be slower. Specifically, we can adjust the value of λ in equation (3). Decreasing the value of λ, which means that the decreasing extent of trust value is much larger than the increasing extent, can prevent strategy nodes from gaining benefits.

Imputation attacks and boosts attacks

If some honest nodes are slandered by some malicious ones, their STV will decrease to quite a low level. Therefore, reputation model should be able to offer nodes the chance to regain their STV. Meanwhile, the request trust value of malicious nodes will decrease accordingly. In this way, when request trust value of malicious nodes decreases to some threshold, there are no nodes which would like to respond to them in networks. In this way, the requests of malicious nodes will be constrained, and malicious nodes would not dare to defame other nodes.

It's not comprehensive to accumulate the trust value based on only a few transactions with nodes, because boost attacks will be easy to come up among a few nodes. Therefore trust evaluation should be collected deep and extensively (Wang, Mokhta, et al., 2008). According to this idea, if transaction successful times reach out to a given value, the STV updating algorithm will change, that is, increasing extent will be slower. Specifically, we can change the λ_1 in equation (1) into $\lambda_1 \times 1/n$ (n stands for transaction successful times between two nodes) to control the deep collection of trust information.

Collusion attacks

Collusive nodes always cooperate with each other (for instance, virtual transactions) to increase their trust value, and organize together to slander other nodes with higher STV. This kind of "teamwork" attack is more harmful than single imputation or boost attack. However, since what we discuss in this chapter is logic network where information is transmitted in flooding; login server automatically creates logical neighbours for new-

joining nodes and randomly distributes them to other nodes as neighbours, a collusion group is hard to form between nodes, which can restrict collusion attacks to some extent.

Sybil attacks (Douceur &Donath, 2002**) and Newcomer attacks (**Resnick & Zeckhauser, 2000**)**

A malicious node can make Sybil attacks to reputation model by pretending to be different nodes in networks with different IDs each time. In this way, different IDs can share the decreasing of trust value so that a single ID of malicious node suffers less punishment.
If a malicious node can easily join in a network as a fresh one, it will delete its bad trust records by frequently entering and leaving the network. This is so-called Newcomer attacks. Two schemes as below can resolve these two kinds of attacks.
Scheme 1: Login server needs some evidences to ensure that each node has one system ID. To keep login server from being open to attacks, such as DoS attack, the function of login server should be decentralized. However, fewer users would like to login if authentic and sensitive information is required. If we just bind the IP address with node ID instead of using login server, sybil attacks will be hard to fight against. SybilGuard (Yu, Kaminsky, et al., 2008) can be seen as a reference, for Yu et al. have proposed an effective protocol to wipe off "attack edge".
Scheme 2: This chapter mainly focuses on reputation model, not only encouraging new-joining nodes but also preventing newcomer attacks. Therefore, we can adopt a mechanism that nodes trust value can slowly reach a certain level which is not too high, if they succeed in previous transactions with a given number. When malicious nodes find it difficult to gain as much benefit as new-joining ones, newcomer attacks will be reduced. For example, a node trust value can finally reach the highest trust value 0.6 after previous 10 successful transactions, while the trust value is easy to drop once nodes process malicious behaviour.

Free riding attacks

There are some nodes referred as free riders in networks. They only receive the service provided by other nodes, but are not willing to provide any service or trust evaluation for other nodes. In our reputation model, the service and request trust value of these nodes all maintain at an initial level, so they can only get very limited resources. In addition, the incentive mechanism (for example, they can obtain the priority of network resources if STV reaches out to some extent) can be adopted in this model to motivate free riders to provide service and trust evaluation.

5. Performance evaluation

To verify the effectiveness of our reputation model, we presented a Java-based simulation program. We firstly checked whether the updating algorithm of trust value can control the STV of strategy nodes. Subsequently, we compared the dual trust values of nodes with expected values when malicious nodes existed in networks. At last, we analyzed how our model resisted the boost attacks.
In simulation environment, we adopted Gnutella routing architecture, with a central server storing trust value. There are totally 1000 nodes and 100 resources in simulation network and each node randomly chooses at most 5 nodes as neighbors and obtains 5 resources. The proportion of malicious nodes is not more than 50%. Averagely, each node sends 100 requests and the Time To Live (TTL) of resource request is 3. We assume that malicious nodes are always the most active ones to respond to any resource request messages. Besides, we also suppose that honest nodes provide honest service and evaluations while malicious

nodes provide fake resources and evaluations. The other common parameters for all the simulation are listed in Table 1. The results are the mean value from several simulations, demonstrated from Fig. 7 to Fig. 12.

Parameters	Description	Default
λ	Ratio of increasing extent to decreasing extent	1/8
λ_1	Trust value increasing extent	0.1
λ_2	Trust value decreasing extent	0.8

Table 1. Simulation Settings

Experiment 1: When all the nodes in network are honest nodes except one strategy node, we observed the change of STV of that strategy node, as is shown in Fig. 7.

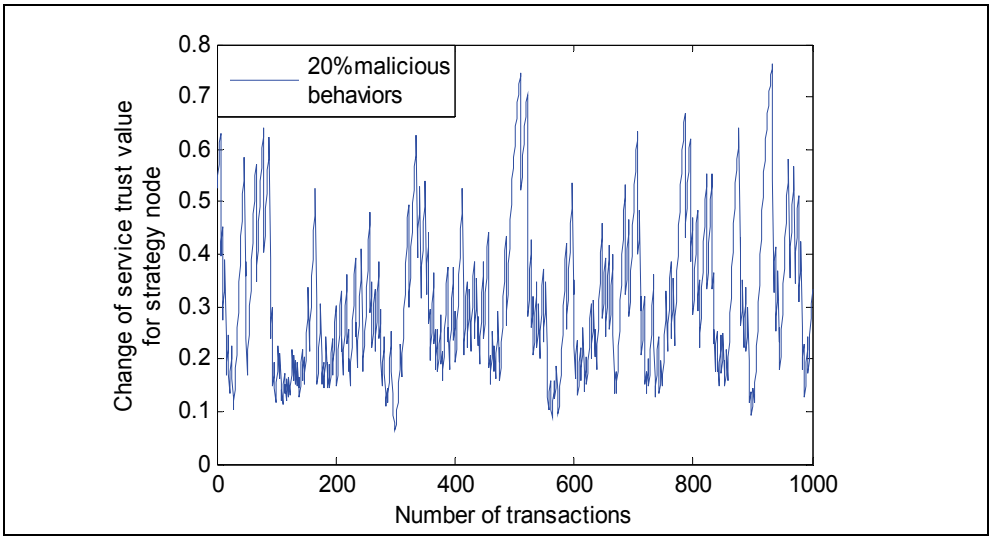


Fig. 7. Changes of STV for Strategy Nodes

In Fig. 7, when strategy node had 20% malicious service, the trust value of that node was controlled at 0.3, at most 0.75. In this case, the strategy node failed to be trusted by resource requester, which made less effect of malicious service on network.

Experiment 2: We set the network with about 30% malicious nodes and 70% honest nodes, and defined that no request could be provided when the RTV of nodes was less than 0.2. Afterwards, we run the updating algorithm of trust value to update dual trust value. After 100000 transactions, we checked whether the STV and RTV of both malicious and honest nodes were within the expected range. The results are presented from Fig. 8 to 10.

Fig. 8 indicates all the STVs of malicious nodes decreased to less than 0.5, which means honest nodes no longer chose these malicious nodes as cooperators. In Fig. 9, all the RTVs of malicious nodes reached 0.195, which was less than 0.2. In this way, these malicious nodes failed to request service. From Fig. 10 we can see that the STV of a minority of honest nodes dropped to 0.5 or less due to imputation attacks from malicious nodes. However, most of

honest nodes became trustful nodes, whose STVs approached 1. For those honest nodes whose trust values decreased, our reputation model allowed them to regain the opportunities to be trusted by offering some new services. Fig. 11 shows that the RTV of honest nodes were all more than 0.5, which means that malicious nodes, as responding nodes, could be controlled after a few transactions, and could not be selected by honest nodes again. Thus the effect was less on the RTV of honest nodes.

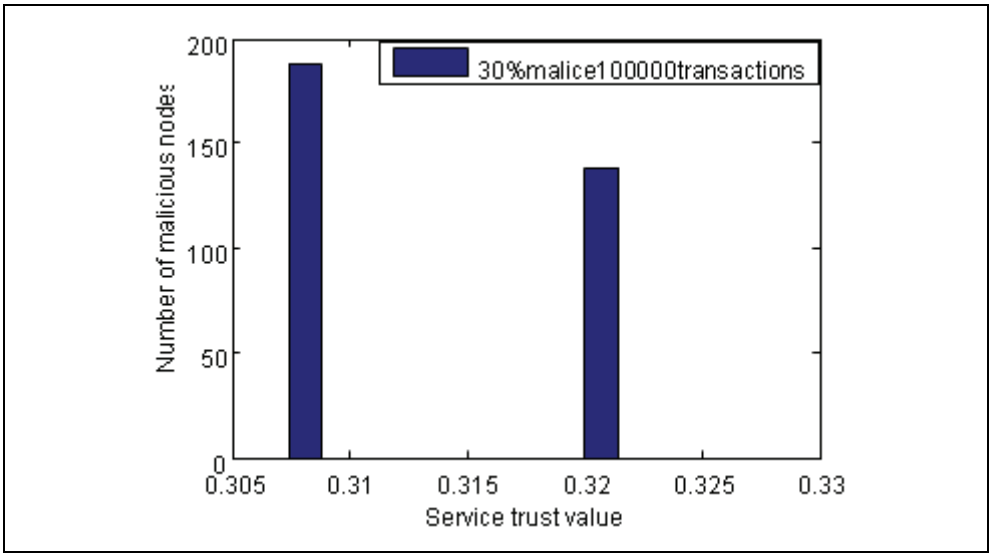


Fig. 8. STV Distribution of Malicious Nodes

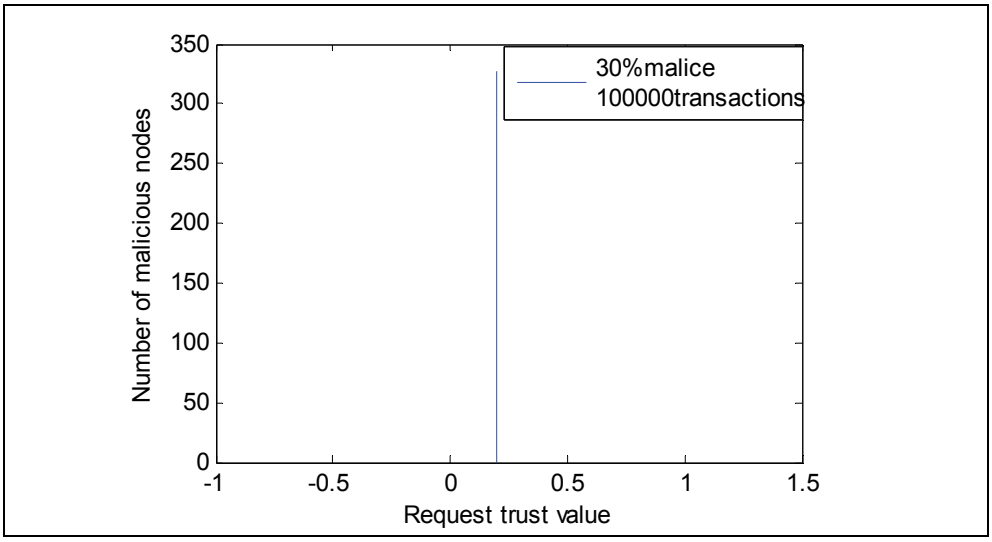


Fig. 9. RTV Distribution of Malicious Nodes

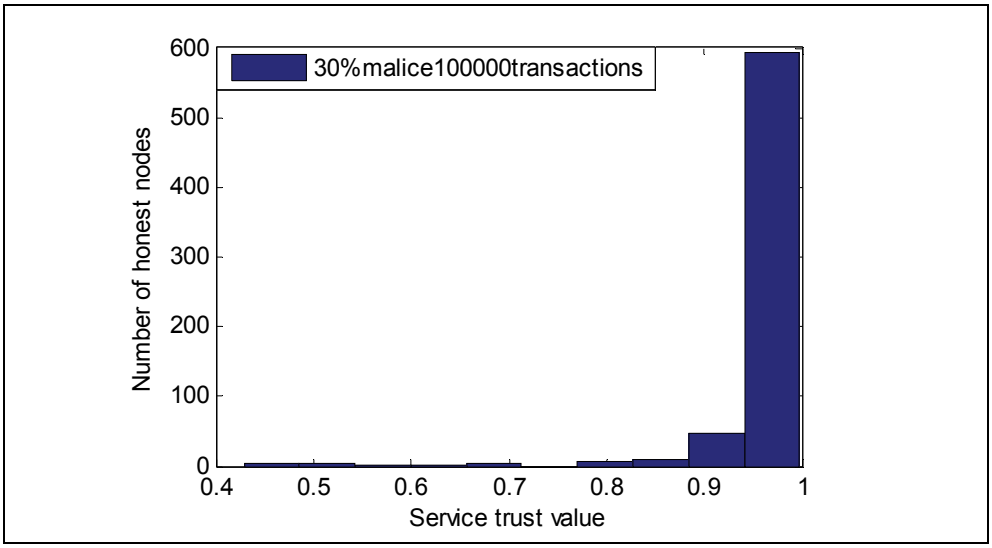


Fig. 10. STV Distribution of Honest Nodes

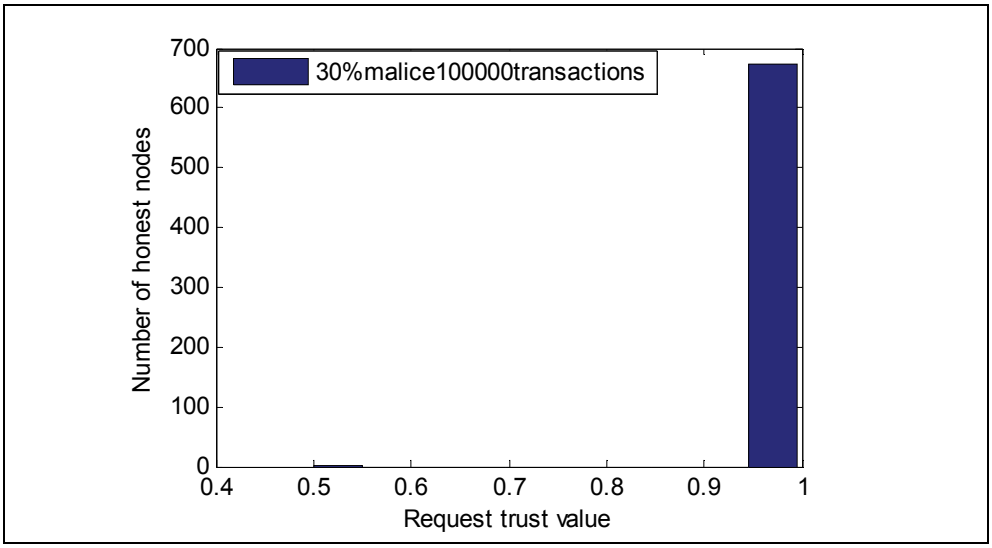


Fig. 11. RTV Distribution of Honest Nodes

Experiment 3: Boost attacks among the nodes in the network will degrade the network performance, causing more damages when happen among malicious nodes. Furthermore, boost attacks can make the STV of malicious nodes rise, hence deceiving honest nodes to transact with them. To avoid this attack, we adopted the updating algorithm with changing λ_1 into $\lambda_1 \times 1/n$. After experiments, we analyzed the changes of STV of some nodes in three conditions: non-boost, 80% boost and 100% boost, as shown in Fig. 12.

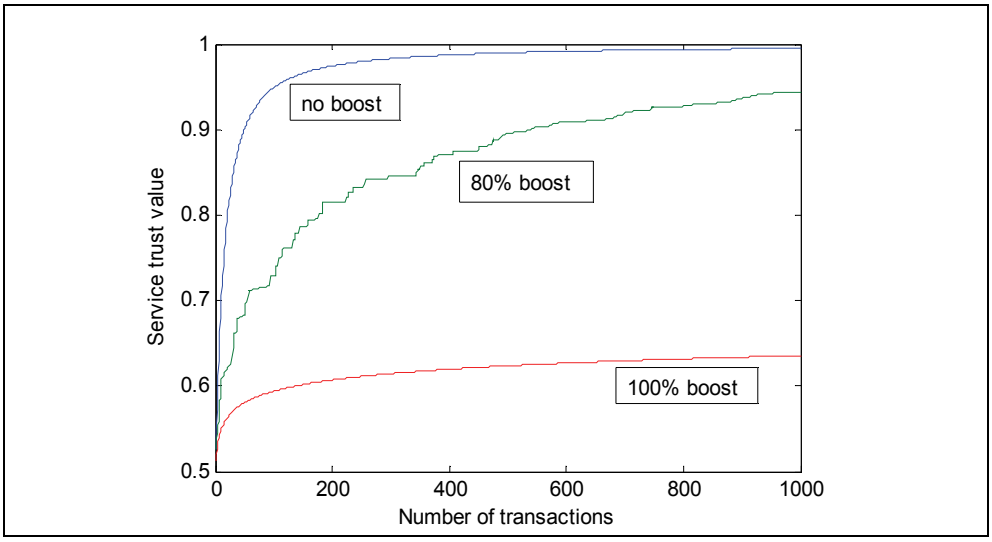


Fig. 12. Comparison of STV for Boost and Non-boost Cases

Fig. 12 illustrates the STV of that node rose slowly in condition of 80% boost, compared with the condition of non-boost. If requesting the same service, this node was selected as service provider. However, due to some honest transactions, the STV can also reach relatively high level after 1000 transactions. On the other hand, we can also see that the STV of malicious nodes in 100% boost achieved 0.6 or so. Once this node responded to honest nodes and is selected as service provider, its STV dropped to less than 0.5 right away. The comparison among these three conditions indicates that our model can effectively resist boost attacks to a certain extent.

6. Discussions and future work

Recommendation mechanism is an important component in any trust evaluation systems. The effectiveness of recommendation is closely related with communication overhead. For example, at the beginning of trust evaluation when few interactions have taken place in the network, higher mobility requires higher overhead. Then, after the trust evaluation system has been running for a long time, a mobile node has had opportunities to interact with many other nodes. Compared with a stationary node, a mobile node has a larger probability to interact with recommenders. In this case, the overhead of requesting recommendations for a node with high mobility can be reduced.

On the other hand, since trust evaluation can effectively improve network performance and detect malicious nodes, trust evaluation itself is an attractive target for attackers (Marmol & Penez, 2009).

A well-known attack is bad-mouthing attack (Dellarocas, 2000), that is, malicious parties providing dishonest recommendations to frame up good parties and/or boost trust values of malicious peers. The defense against the bad-mouthing attack has been considered in the design of the proposed trust evaluation system. First, the action trust and the recommendation trust records are maintained separately. Only the nodes who have provided good recommendations previously can earn high trust. Second, according to the

necessary conditions of trust propagation, only the trust from the entities with positive trust can propagate. Third, the fundamental axioms limit the power of the entities with low trust.
Trust evaluation may also be vulnerable to the Sybil attack and the newcomer attack. If a malicious node can create several faked IDs, the trust evaluation system suffers from the Sybil attack. Here, the faked IDs can share or even take the blame, which otherwise should be given to the malicious node. If a malicious node can easily register as a new user, the trust evaluation suffers from the newcomer attack. Here, malicious nodes can easily remove their bad history by registering as a new user. The defense against the Sybil attack and newcomer attack does not rely on the design of trust evaluation system, but the authentication and access control mechanisms, which make registering a new ID or a faked ID difficult.
In terms of security issues in trust model, some literatures related to our work have done a lot researches in trust mechanism. Here I will compare some typical models with our work in detail.
S. F. Peng, et. al. showed a weighted trust formula and presented an integrated trust update method. They used abnormal trust value sequence and statistical analysis to detect malicious recommenders and false recommendation trust values in the whole lifetime of trust. In addition, trust value update analysis aims at protecting against untrue recommendation, such as the collusion problem. However, authors adopted a common formula $T(n, m) = \alpha \times T_d + (1-\alpha) T_r$ to do the trust evaluation, which is different from our model. Meanwhile, the update of α was not considered in the paper, so we do not know the impact of α on trust formalization when it changes.
P. Victor, et. al. advocated the use of a centralized trust model in which trust scores are (trust, distrust)couples, drawn from a bilattice that preserves valuable trust provenance information including gradual trust, distrust, ignorance, and inconsistency. Authors presented a collection of four operators simultaneously in one model, especially the distrust information, which is their novel contribution. However, proposed trust techniques require a central authority to propagate and aggregate trust values; however, as the amount of nodes continues to grow, it will get more and more difficult to manage all trust information in one place, so a decentralized approach may be more appropriate. Furthermore, privacy of data is becoming increasingly important in applications, and nodes may refuse to disclose their personal trust. Authors didn't discuss the security issues in the paper.
J. H. Luo, et. al. promoted RFSTrust, a trust model based on fuzzy trust similarity to quantify and to evaluate the trustworthiness of nodes, which includes five types of fuzzy trust relationships based on the fuzzy relation theory and a mathematical description for MANETs. RFSTrust has some identification and containment capability in synergies cheating, promotes data packets forwarding between nodes, and improves the performance of the entire MANETs. But authors discuss only one type of situation when selfish nodes attack. No other types of nodes attacks are considered.
J. S. Liu and V. Issarny presented a reputation model, which incorporates two essential dimensions, time and context, along with mechanisms supporting reputation formation, evolution and propagation. Their model shows effectiveness in distinguishing truth-telling and lying agents, obtaining true reputation of an agent, and ensuring reliability against attacks of defame and collusion. The common ground of their work and ours is that we both take the time dimension of trust update into consideration, while the main difference is that Liu regards node's new behavior as a part of trust value, while we see the service and request from other nodes as a key proportion of trust establishment.
X. M. Li, et. al. gave us a global trust model, which is based on the distance-weighted recommendations under P2P circumstance (Li & Wang, 2009). Their model uses distributed

methods to quantify and evaluate the credibility of peers to identify and restrain some common collective cheatings. The global credibility relies on distance between nodes in their model, and Distributed Hash Table (DHT) is used to designate peers to mange the credibility. That is to say, hash function needs using in their model, which is different from ours.
Besides these known attacks in the literatures, a malicious node may also reduce the effectiveness of trust evaluation through other methods. While the focus of this chapter is to lay the foundation of trust evaluation with meaningful trust metrics, we do not investigate all possible attacks in this chapter. Therefore, more security issues of cooperative communication in Ad Hoc networks are our following targets.

7. Conclusion

The creditability of multi-hop networks can achieve from the aspects of authentication, authorization, access control, as well as the reputation-based trust management model (Wang & Lin, 2008). In this chapter we propose a reputation model based on global STV and RTV. Afterwards, we discuss five attacks on the model in the progress of establishing reputation, and testify the model robustness of anti-attacks by simulations. Since the proposed model takes no consideration of the location issue of nodes for computing and storing trust information, our model can be applied in both structured multi-hop networks and unstructured ones.

8. Acknowledgements

We acknowledge a financial support from Six Talented Eminence Foundation of Jiangsu Province(06-E-043); Scientific Research Foundation of NJUPT (NY209016);

9. References

Aameek, S. & Liu, L. (2003). TrustMe: anonymous management of trust relationships in decentralized P2P systems, *Proceedings of IEEE 3rd International Conference on Peer-to-Peer Computing*, pp. 142-149, ISBN: 0-7695-2023-5, Sweden, September 2003, IEEE Press, Linkoping

Boukerche, A. & Ren, Y. L. (2008). A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications*, Vol. 31, No. 18, page numbers (4343-4351), ISSN: 0140-3664

Buchegger, S. & LeBoudec, J. Y. (2002). Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes-Fairness in Dynamic Ad-Hoc NeTworks, *Proceedings of the 3rd ACM International Symposium of Mobile MANET Networking and Computing*, pp. 80-91, ISBN: 1-58113-501-7, Switzerland, June 2002, ACM Press, Lausanne

Caronni, G. (2000). Walking the Web of trust, *Proceedings of the IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 153-159, ISBN: 0-7695-0798-0, USA, June 2000, IEEE Press, MD

Chang,B. J. & Kuo, S. L. (2009). Markov Chain Trust Model for Trust-Value Analysis and Key Management in Distributed Multicast MANETs. *IEEE Transactions on Vehicular Technology*, Vo l. 58, No. 4, page numbers (1846-1863), ISSN: 0018-9545

Dellarocas, C. (2000). Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems, *Proceedings of the Intenational Conference on Intelligent Systems*, pp. 520-525, ISBN: ICIS2000-X, Australia, December 2000, AIS Press, Brisbane, Queensland

Ding, X. H. ; Yu, W. & Pan, Y. (2008). A Dynamic Trust Management Scheme to Mitigate Malware Proliferation in P2P Networks, *Proceedings of IEEE International Conference on Communication*, pp. 1605-1609, ISBN: 978-1-4244-2075-9, China, May 2008, IEEE Press, Beijing

Douceur, J. R. & Donath, J. S. (2002). The sybil attack, *Proceedings of the first International Workshop on Peer-to-Peer systems*, pp. 251-260, ISBN: 3-540-44179-4, USA, March 2002, Springer-Verlag Press, MIT Faculty Club, Cambridge, MA

ElSalamouny, E. ; Krukow, K. & Sassone, V. (2009). An analysis of the exponential decay principle in probabilistic trust models. *Theoretical Computer Science*, Vol. 410, No. 41, page numbers (4067-4084), ISSN: 0304-3975

Frank, H. P. F. & Marcos, D. K. (2006). Cooperation in Nature and Wireless Communications, In: *Cooperation in Wireless Networks: Principles and Applications*, Frank, H. P. F. & Marcos, D. K. (Eds.), page numbers (1-27), Springer Press, ISBN: 978-1-4020-4710-7, Netherlands

He, Q. & Wu, D. (2004). SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks, *Proceedings of IEEE Conference on Wireless Communications and Networking*, pp. 825-830, ISBN: 0-7803-8344-3, USA, March 2004, IEEE Press, Atlanta, GA

Jin, Y. ; G, Z. M. & B, Z. J. (2007). Restraining False Feedbacks in Peer-to-Peer Reputation Systems, *Proceedings of International Conference on Semantic Computing*, pp. 304-312, ISBN: 0-7695-2997-6, USA, September 2007, IEEE Press, CA

Kamvar, S. D. ; Mario, T. S. & Molina, H. G. (2003). The EigenTrust Algorithm for Reputation Management in P2P Networks, *Proceedings of the 12th International Conference on World Wide Web*, pp. 640-651, ISBN: 1-58113-680-3, Hungary, May 2003, ACM Press, Budapest

Li, X. & Liu, L. (2004). PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Transactions on Knowledge and Data Engineering*, Vol. 16, No. 7, page numbers (843-857), ISSN: 1041-4347

Li, X. M. & Wang, J. K. (2009). A Global Trust Model of P2P Network Based on Distance-Weighted recommendation, *Proceedings of 2009 IEEE Intenational Conference on Networking, Architecture, and Storage*, pp. 281-284, ISBN: 978-0-7695-3741-2, China, July 2009, IEEE Press, Zhang Jia Jie, Hunan

Liu,J. S. & Issarny, V. (2004). Enhanced Reputation Mechanism for Mobile Ad-hoc Networks, *Proceedings of 2nd International conference on Trust Management*, pp. 48-62, ISBN: 3-540-21312-0, UK, March 2004, Springer Press, Oxford

Luo, J. ; Liu, H. X. & Fan, M. Y. (2009). A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Computer Networks*, Vol. 53, No. 14, page numbers (2396-2407), ISSN: 1389-1286

Ma, X. X. & Qin, Z. G. (2008). Partition and multi-path transmission: An encryption-free reputation sharing protocol in Gnutella-like peer-to-peer network. *Computer Communications*, Vol. 31, No. 14, page numbers (3059-3063), ISSN: 0140-3664

Marmol, F. G. & Perez, G. M. (2009). Security threats scenarios in trust and reputation models for distributed systems. *Computer & Security*, Vol. 28, No. 7, page numbers (545-556), ISSN: 0167-4048

Marti, S. & Molina, H. G. (2006). Taxonomy of Trust: Categorizing P2P Reputation Systems. *Computer Networks*, Vol. 50, No. 4, page numbers (472-484), ISSN: 1389-1286

Michiardi, P. & Molva, R. (2002). Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks, *Proceedings of IFIP - Communication*

and Multimedia Security, pp.107-121, ISBN: 1-4020-7206-6, Slovenia, September 2002, Kluwer Press, Portoroz

Millan, G. L.; Perez, M. G.; Perez, G. M. & Skarmeta, A. F. G. (2010). PKI-Based Trust Management in Inter-Domain Scenarios. *Computers & Security*, Vol. 29, No. 2, page numbers (278-290), ISSN: 0167-4048

Omar, M. ; Challal, Y. & Bouabdallah, A. (2009). Reliable and fully distributed trust model for mobile ad hoc networks. *Computers & Security*, Vol. 28, No. 3, page numbers (199-214), ISSN: 0167-4048

Ozdemir, S. (2008). Functional reputation based reliable data aggregation and transmission for wireless sensor networks. *Computer Communications*, Vol. 31, No. 17, page numbers (3941-3953), ISSN: 0140-3664

Paola, D. & Tamburo, A. (2008). Reputation Management in Distributed Systems. *Proceedings of the 3rd International Symposium on Communications, Control and Signal Processing*, pp. 666-670, ISBN: 978-0-7695-3258-5, March 2008, Malta

Peng, S. F. ; He, J. S. & Meng Y. (2008). Reputation-based Trust update in network environment, *Proceedings of 2008 International Symposium on Electronic Commerce and Security*, pp. 118-123, ISBN: 978-0-7695-3258-5, China, August 2008, IEEE Press, Guangzhou

Resnick, P. & Zeckhauser, R. (2000). Reputation System. *Communications of the ACM*, Vol. 43, No. 12, page numbers (45-48), ISSN: 0001-0782

Saurabh, G. ; Laura, K. B. & Mani, B. S. (2008). Reputation-based framework for high integrity sensor networks. *ACM Security for Ad-hoc and Sensor Networks*, Vol. 4, No. 3, page numbers (1-17), ISSN: 1550-4859

Sun, Y. ; Zhu H. & Liu, K. J. R. (2008). Defense of Trust Management Vulnerabilities in Distributed Networks. *IEEE Communications Magazine*, Vol. 46, No. 2, page numbers (112-119), ISSN: 0163-6804

Thomas, R. & Vana, K. (2006). Decentralized trust management for ad-hoc peer-to-peer networks, *Proceedings of the 4th international workshop on Middleware for Pervasive and Ad-Hoc Computing*, pp. 6, ISBN: 1-59593-421-9, Australia, November 2006, ACM Press, Melbourne

Victor, P.; Cornelis, C. ; De Derk, M. & Silva, P. P. (2009). Gradual trust and distrust in recommender systems. *Fuzzy Sets and Systems*, Vol. 160, No. 10, page numbers (1367–1382), ISSN: 0165-0114

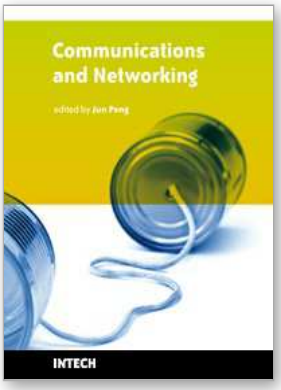
Wang, W. G.; Mokhta, M. & Linda, M. (2008). C-index: trust depth, trust breadth, and a collective trust measurement, *Proceedings of the hypertext 2008 workshop on Collaboration and collective intelligence*, pp. 13-16, ISBN: 978-1-60558-171-2, USA, June 2008, ACM Press, Pittsburgh, PA

Yu, B.; Singh, M. P. & Sycara, K. (2004). Developing trust in large-scale peer-to-peer systems, *Proceedings of IEEE First Symposium on Multi-Agent Security and Survivability*, pp.1-10, ISBN: 0-7803-8799-6, USA, August 2004, IEEE Press, PA

Yu, H. F.; Kaminsky, M. ; Gibbons, P. B. & Flaxman, A. D. (2008). SybilGuard: Defending Against Sybil Attacks via Social Networks. *IEEE/ACM Transactions on networking*, Vol. 16, No. 3, page numbers (576-589), ISSN: 1-59593-308-5

Zhang, Y. C. & Fang, Y. G. (2007). A Fine-Grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 18, No. 8, page numbers (1134-1145), ISSN: 1045-9219

Zhou R. F. & Hwang, K. (2007). PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 18, No. 4, page numbers (460-473), ISSN: 1045-9219



Communications and Networking

Edited by Jun Peng

ISBN 978-953-307-114-5
Hard cover, 434 pages
Publisher Sciyo
Published online 28, September, 2010
Published in print edition September, 2010

This book "Communications and Networking" focuses on the issues at the lowest two layers of communications and networking and provides recent research results on some of these issues. In particular, it first introduces recent research results on many important issues at the physical layer and data link layer of communications and networking and then briefly shows some results on some other important topics such as security and the application of wireless networks. In summary, this book covers a wide range of interesting topics of communications and networking. The introductions, data, and references in this book will help the readers know more abut this topic and help them explore this exciting and fast-evolving field.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Kun Wang, Meng Wu and Subin Shen (2010). Secure Trust-based Cooperative Communications in Wireless Multi-Hop Networks, Communications and Networking, Jun Peng (Ed.), ISBN: 978-953-307-114-5, InTech, Available from: http://www.intechopen.com/books/communications-and-networking/secure-trust-based-cooperative-communications-in-wireless-multi-hop-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821