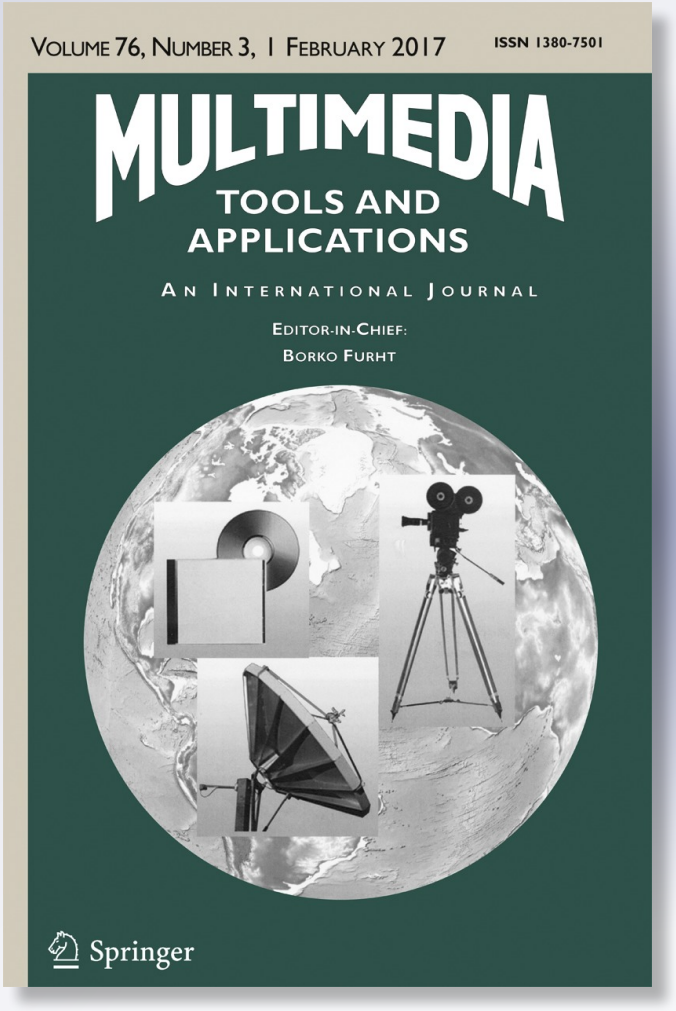
A service recovery method based on trust evaluation in mobile social network

Danmei Niu, Lanlan Rui, Haoqiu Huang & Xuesong Qiu

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501
Volume 76
Number 3

Multimed Tools Appl (2017)
76:3255-3277
DOI 10.1007/s11042-016-3963-4



Springer

Your article is protected by copyright and all rights are held exclusively by Springer Science +Business Media New York. This e-offprint is for personal use only and shall not be self-archived in electronic repositories. If you wish to self-archive your article, please use the accepted manuscript version for posting on your own website. You may further deposit the accepted manuscript version in any repository, provided it is only made publicly available 12 months after official publication or later and provided acknowledgement is given to the original source of publication and a link is inserted to the published article on Springer's website. The link must be accompanied by the following text: "The final publication is available at link.springer.com".

Author's personal copy

Multimed Tools Appl (2017) 76:3255–3277
DOI 10.1007/s11042-016-3963-4

A service recovery method based on trust evaluation in mobile social network

Danmei Niu[1,2] · Lanlan Rui[1] · Haoqiu Huang[1] · Xuesong Qiu[1]

Received: 14 January 2016 / Revised: 7 September 2016 / Accepted: 14 September 2016 /
Published online: 27 September 2016
© Springer Science+Business Media New York 2016

Abstract Mobile social network makes users create and share multimedia contents freely and conveniently. However, some nodes in mobile social network have malicious behavior, such as discarding or tampering packet. These factors will cause service interruptions in the process of providing multimedia contents for the user. When the service interruption happens, how to choose the more reliable backup device, reduce interruption number, increase the packet transmission efficiency and improve user's experience of sharing multimedia contents is the object of this paper. We propose a service recovery method based on trust evaluation which adopts Dempster-Shafer (D-S) evidence theory. The service requester calculates the direct trust degree and the recommended trust degree of the backup devices, then uses the evidence combination rule to calculate the comprehensive trust degree. The backup device with the highest trust value will be seclected to recover the service. The simulation results show that this method effectively improves the packet delivery ratio, reduces the service execution time and provides users with more stable multimedia contents.

✉ Danmei Niu
niudanmei@163.com

Lanlan Rui
llrui@bupt.edu.cn

Haoqiu Huang
francesco@bupt.edu.cn

Xuesong Qiu
xsqiu@bupt.edu.cn

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

[2] Information Engineering College, Henan University of Science and Technology,
Luoyang 471023, China

Author's personal copy

Keywords Multimedia content · Service recovery · Trust evaluation · Mobile social network

1 Introduction

The emergence of social network greatly expands people's social scope and reduces the cost of communications. In recent years, with the rapid development of wireless network and smart mobile phone, users can use social network when they are in outdoor activities or tourism. Friends, families, colleagues and classmates can communicate, spread and share multimedia contents (such as texts, pictures, audios, videos and geographic position, etc.) anytime and anywhere, which is not limited to a special place and prompts the emergence of mobile social network [16, 27, 29].

Mobile social network is a virtual interactive community based on wireless network service. It is made up of interconnected devices including smart phones, tablets, laptops and other wireless devices, which belong to people with certain social relations [10]. Compared with the traditional social network service, mobile social network service has the characteristics of human-computer interaction and real-time scene and is able to make users create and share multimedia contents freely [5, 15, 28]. Mobile social network has the advantage of transmitting multimedia contents directly, quickly and flexibly.

Mobile social network can be divided into three types. The first type is the traditional social website open to the users with mobile devices. The second type is the social network consists of mobile application programs (App) providing interactive function and interest division service. The third type is the mobile social network similar to mobile ad-hoc network (MANET), which divides the mobile users according to the same or similar features and forms self-organizing mobile social network [6, 25]. The mobile social network discussed in this paper is the third one.

Due to the openness of the network, mobile social network is vulnerable to malicious or selfish nodes. In order to reduce the harm of these nodes, ensure users' service experience of sharing multimedia contents and build secure and reliable mobile social network, this paper puts forward a service recovery method based on trust evaluation.

Trust is one of the most complicated concepts in the social relations and is a psychological cognitive process, involving assumption, expectation, behavior, environment and other factors. Similar to human society, a person will request others to finish some tasks if trust them. Trust is applied to different research fields, such as trusted computing, trusted code and trust management. However, the secure methods based on identity authentication or cryptography cannot handle internal malicious or selfish nodes.

In this paper, trust is the measurement of nodes' ability to provide required service including providing multimedia contents and transmitting data. Trust mechanism is able to judge whether the node is malicious or selfish node and makes sure the service quality of a node. Then the trust mechanism provides the corresponding access control according to the specific circumstance and decides how to establish safe and reliable routing. When the service interrupts, the mechanism selects the node with the highest trust degree to continue to fulfill the task of providing multimedia contents, thus ensures the robustness and reliability of the service.

The remaining of this paper is organized in the following manner. Section 2 examines related studies. Section 3 describes the problem in detail. Section 4 evaluates the trust degree of the backup device based on D-S evidence theory. Section 5 presents the algorithm of the recovery method. Section 6 shows the simulation experiments

Author's personal copy

and result analysis. Finally, Section 7 provides the conclusions and suggests the future work.

2 Related work

In mobile social network, users can establish groups based on some relationship which includes families, friends, common interests or participating in activities. They will communicate and share multimedia contents within or between the groups. If the malicious behavior or malfunction of a device node occurs, it will cause multimedia services providing for the users interruptions. How to select the backup devices based on trust evaluation for service recovery is the main problem in this paper. This paper mainly investigates three aspects of literature including the community division of mobile social network, the service recovery of wireless network and the trust model.

Yang et al. [25] present a distributed mobile communications system referred to as E-SmallTalker that facilitates social network in physical proximity. It automatically discovers and suggests topics such as common interests for more significant conversations. Based on E-SmallTalker, mobile users interact related information through Bluetooth technology, match information and find the topics of common interests.

Boix et al. [6] introduce a user application named Flocks based on mobile social network. This reference puts forward a model with asynchronous interaction which facilitates users' interaction with similar semantic contents and close geographic position. It constructs communities based on users' social relationship and physical locations.

In the current researches of service recovery of wireless network, some researches recover service according to the performance of the devices. Sun et al. [20] present cold backup service replacement strategy (BSRS) and hot backup service replacement strategy (HBSRS). In BSRS, each node executes service in sequence according to the user's requirements. When a service node fails, the strategy sorts the available backup nodes with an algorithm. The node with the highest priority will be selected. In HBSRS, the backup service nodes are sorted continually whether or not the service interrupts. The backup node is ready to replace the failing node at any time. Compared with BSRS, HBSRS reduces repair time, but increase the cost. However, the reference does not specify how to calculate the priority of the backup service nodes.

A typical recovery method for wireless or dynamic network is resend request strategy(RRS) [7, 8]. A service is divided into several atomic services. The user selects some of the atomic services to constitute. When the composite service interrupts, the service requester will resend a request. In the process of re-executing service composition, caching technology is used to ensure the service quality. However, the dynamic network topology is unstable, some services provided by devices will never be used. If the service requester or service provider is always in a wait state, the network load and service execution time will greatly increase, and the availability and reliability of service cannot be guaranteed.

In distributed, heterogeneous and autonomous network, constructing trust relationship between different users is an important research problem [21], especially when users interact and share services. Trust may contain different aspects, such as intimacy, reliability, collaboration, security, ability and cost, etc. Trust relationship is the basis of the transaction between users, and the evaluation of trust intensity is a complex model of decision-making system based on multiple elements. So the research of trust degree is of great significance. Trust degree can serve as the basis of service scheduling and binding, which will improve

Author's personal copy

the service reliability, reduce the frequency of service interruptions and benefit the devices collaboration.

About trust evaluation and model, Li et al. [13] put forward a global trust evaluation algorithm used to composite service selection and discovery in serviced-oriented computing (SOC) environments. But this reference calculates the trust value of service scheduling flow according to the pre-defined value for each service. The idea is simple and not suitable for the actual environments.

Bao et al. [3] propose hierarchical trust management protocol used in wireless sensor network. The sensor nodes in a cluster evaluate each other and report the results to their cluster heads. The cluster heads evaluate each other and report the results to the base station. Finally, the base station finishes the trust evaluation of all the cluster heads. Whether a sensor node is reliable can be judged from the combination of trust values.

Similar to [3], Shaikh et al. [19] put forward a group-based trust management scheme (GTMS) for wireless sensor network, which employs clustering. The sensor nodes in a cluster evaluate each other and report the results to their cluster heads. The cluster heads evaluate each other and report the results to the base station. A sensor node is trusted if its trust value exceeds the threshold. The simulation results demonstrate that the scheme reduces power and memory consumption. In [3, 19], all the sensor nodes and the cluster heads evaluate others periodically and report the results to their superiors. It will greatly cost the nodes and network resources, especially for the sensor nodes whose power, memory and computation ability are very limited.

Xia et al. [22] present a trust prediction model for MANET which uses the fuzzy logic rules prediction method to calculate the trust value of the nodes. The model provides the correct prediction of the future behavior of nodes. Based on the model, the reference proposes a trust-based source routing protocol (TSR). The source node may construct multiple routings to the destination. In the process of routing discovery, each routing will be calculated a trust value. The routing selection is on the basis of the routing trust value. Some assumptions of this method are too idealistic, sometimes are not suitable for the actual network situation.

Aivaloglou et al. [1] propose a hybrid trust model for sensor network, the trust relationship between the two nodes consists of several trust evidence including the local information before nodes deploying, the nodes' effective certificate, the recommendation trust of the third part and the behavior trust evaluation from the monitor, etc. If a node wants to evaluate others, it needs to collect too much trust evidence. The collecting progress is complicated, but the power, memory and computing ability of a sensor node are very limited. In addition, saving the key increases the network security risk.

In summary, most of the researches on trust degree are related to the trust relationship between users. However, few researches focus on how to apply trust evaluation and measurement to service recovery. Based on the study of the community division of mobile social network, the service recovery and the trust model, this paper presents a service recovery method based on trust evaluation in mobile social network.

3 Problem description

In mobile social network, users can establish groups based on some relationship and communicate and share multimedia contents within or between the groups. The users are divided into multiple groups according to their interests and geographic location in this paper. Suppose there is such a scenario, some travelers, for example, classmates of one or several classes of a college go into tourist area. The social relationship of the classmates in a group

Author's personal copy

is stable. All the travelers carry some mobile devices including mobile phone, laptop or tablet computer, etc. Because the mobile devices are dynamic, the community division of mobile social network needs to consider the users' geographic locations. Here, community division means dividing the users according to the same or similar features and forming self-organizing mobile social network.

In this paper, suppose the classmates in a group are close in distance. These classmates are the users who usually move with the common object and direction in a group. The users share multimedia contents including geographic location, text, pictures, music and video with the mobile devices in a group. This paper assumes that the traveling or exploring scenic area is large mountain or virgin forest area and lacks communication infrastructures. The device nodes can share multimedia contents through short distance communication technologies, such as Bluetooth or ad hoc technology. Figure 1 is the network model.

In each group, there is a mobile leader responsible for managing and saving the service for its group members. A group is called cluster, and the leader of a group is called cluster head which is denoted by triangle node in Fig. 1. The mobile devices of a group are called cluster members which are denoted by round nodes.

Suppose in the area lack of communication infrastructures, the cluster head's performance is usually better, memory is bigger and transmission speed is faster. According to different application requirements, several clustering algorithms such as fast clustering, reducing energy consumption or computational overhead and considering load balance have been put forward [2, 4, 17]. These clustering algorithms generally select the suitable cluster heads by considering and comparing the performance of each node. The factors of the

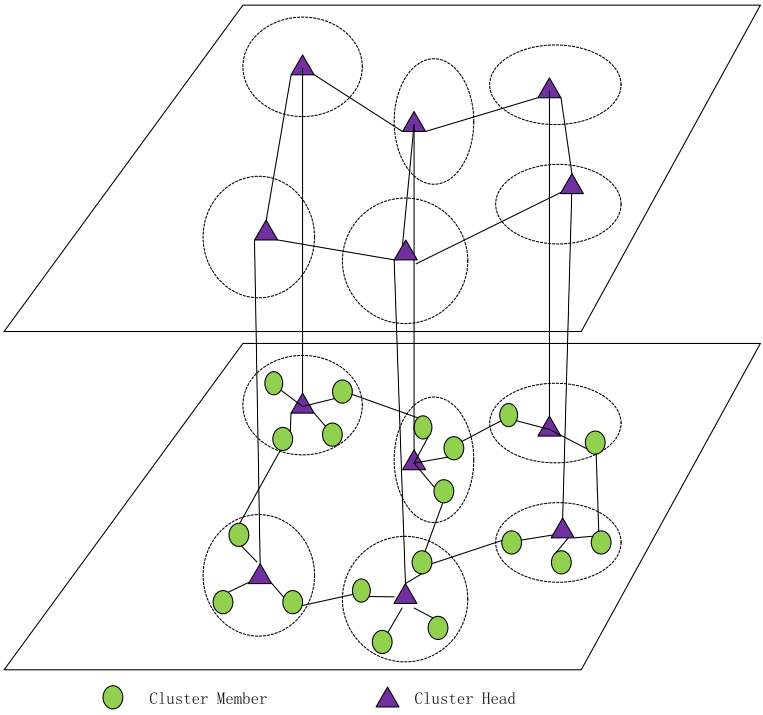


Fig. 1 Network model

Author's personal copy

performance contains electric power, ability to receive network signal, node connectivity, the distance between neighbors, geographic location and average speed, etc. The node with the best evaluation result within a region will be selected as the cluster head. Due to the formation of cluster and the selection of cluster head is not the focus in this article, we do not describe here.

If the cluster head's ability to receive network signal is relatively strong, even in the area of lack of communication infrastructures, the cluster heads communicate by mobile devices. If the network signal is very weak and the cluster heads cannot receive network signal, the cluster heads can communicate by emergency communication devices which are probably mobile satellite phones or satellite data terminals. The mobile satellite phone provides communication services similarly to ordinary mobile communication services. The satellite data terminal has the ability to create Wi-Fi hot spots supporting satellite communication network and provide satellite connection for several mobile devices. Users can enjoy multimedia contents anytime and anywhere conveniently.

Service discovery within a group is done by the cluster head who can establish relationship with other cluster heads. In this way, the multimedia contents are shared by all the group members. The cluster head is responsible for cluster formulation, member joining and leaving, service register and network topology maintaining. Because the power and processing ability of a mobile device is limited, clustering network structure makes the mobile device need not to save the whole network topology. In a large-scale dynamic network, clustering network structure is conducive to effectively guide network traffic and save service discovery time. So it is suitable for the scenario of group traveling or expedition in mobile social network.

If a user needs some multimedia contents, he first sends a service request to the cluster head through the mobile device. The cluster head discovers if there are required multimedia contents. If there are no such contents or not all the multimedia contents are in its cluster, the cluster head will send the service request to other cluster heads. This process is repeated until all the required multimedia contents are discovered. A cluster member can directly send data to the requester within a cluster. But the service provider outside the cluster of requester will send data to the requester according to the request path, and the process perhaps experience transmission by more than one cluster head and relaying node.

Some nodes have malicious behavior, such as discarding or tampering packet. Node mobility or power limitation may cause node failure. These factors will cause service interruptions in the process of providing multimedia contents for the user, which seriously affect the user's experience of sharing multimedia contents. When the service interruption happens, how to choose the more reliable backup device, reduce interruption number, increase the packet transmission efficiency and improve the user's experience of sharing multimedia contents is the main problem in this paper. So we put forward a service recovery method based on trust evaluation in mobile social network.

4 Trust degree evaluation

Trust degree is the comprehensive performance of a mobile node, which means different participants' trust evaluation for the mobile node. These participants in the network include the service requester, the cluster head and the service provider.

Based on Dempster-Shafer (D-S) evidence theory, this paper presents a method of trust degree evaluation. This method does not require any centralized or distributed trusted infrastructures. When some of the devices fail and the service interrupts, the method will decide

Author's personal copy

which backup device is the best candidates according to the trust degree evaluation. Then repair the interrupted links and recover the service quickly. The method of trust degree evaluation is shown in Fig. 2.

4.1 D-S evidence theory

D-S evidence theory is a kind of imprecise evidence reasoning theory which is first proposed by Dempster [9] and developed by his student Shafer [18]. The theory is effective in imprecise evidence processing and information fusion and has been widely applied to deal with uncertain and conflict evidence problems [11]. It extends the concept of probability theory and presents belief function and plausibility function. The core idea of the theory is Dempster's combinational rule. Through this rule, different evidences can be combined together, which leads to a comprehensive result and makes the decision more reliable.

Suppose Θ is an identification frame or hypothesis space. It is a limited set which consists of N repellent and finite basic proposition. A power set $P(\Theta)$ consists of 2^N subsets based on Θ, $P(\Theta) = \{\phi, \{A_1\}, \{A_2\}, \ldots \{A_1, A_2\}, \ldots \Theta\}$. Basic probability assignment (BPA) function $m(A) : P(\Theta) \rightarrow [0, 1]$ is defined based on $P(\Theta)$, which satisfies

$$m(\phi) = 0, \sum_{A \subseteq P(\Theta)} m(A) = 1 \tag{1}$$

BPA function $m(A)$ expresses trust degree to A.

Belief function (Bel) $Bel(A) : P(\Theta) \rightarrow [0, 1]$ expresses trust degree to a set and its subsets,

$$Bel(A) = \sum_{B \subseteq A} m(B), \forall A \subseteq P(\Theta) \tag{2}$$

Plausibility function (Pl) $Pl(A) : P(\Theta) \rightarrow [0, 1]$ expresses the degree of not denying a proposition,

$$Pl(A) = \sum_{A \cap B = \phi} m(B), \forall A \subseteq P(\Theta) \tag{3}$$

Its relationship with Bel satisfies

$$Pl(A) = 1 - Bel(\sim A) \tag{4}$$

$\sim A$ is the negated proposition of A, $Pl(A)$ expresses the degree of not denying A is true.

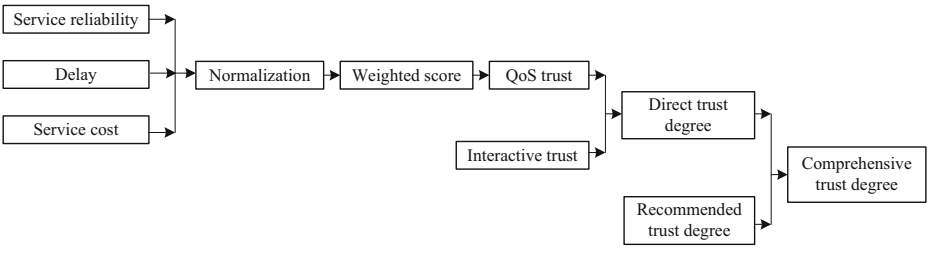


Fig. 2 Method of trust degree evaluation

Author's personal copy

Suppose at the same identification frame Θ , there are $n(n \geq 2)$ repellent and finite evidences whose BPA functions are $m_1, m_2, m_3, \ldots m_n$. According to D-S evidence theory, BPA function of n synthetic evidences $m(A)$ satisfies formula (5).

$$m(A) = (m_1 \oplus m_2 \oplus \ldots \oplus m_n)(A) = \frac{1}{K} \sum_{A_1 \cap A_2 \cap \ldots \cap A_n = A} m_1(A_1) m_2(A_2) \ldots m_n(A_n) \quad (5)$$

$m(\phi) = 0$, and K is a normalized constant which is called conflict factor and satisfies formula (6).

$$\begin{aligned} K &= \sum_{A_1 \cap A_2 \cap \ldots \cap A_n \neq \phi} m_1(A_1) m_2(A_2) \ldots m_n(A_n) \\ &= 1 - \sum_{A_1 \cap A_2 \cap \ldots \cap A_n = \phi} m_1(A_1) m_2(A_2) \ldots m_n(A_n) \end{aligned} \quad (6)$$

When a device providing a multimedia content fails and the service interrupts, there are several methods finding a backup device to replace the failed device and continue providing the multimedia content. This paper adopts trust evaluation method based on D-S evidence theory to evaluate each backup recovery devices. The goal of this paper is to choose the most trustworthy backup device and recover the service as soon as possible.

In order to realize this method, we need to consider two aspects of the trust evaluation of the backup recovery device, one is the direct trust degree and the other is the recommended trust degree.

4.2 Direct trust degree

In this paper, the direct trust degree of a backup recovery device is calculated by the service requester. The value of direct trust degree changes with time. It consists of two parts, one part is quality of service (QoS) trust. This value is the performance evaluation of the device which is expressed by several QoS attribute values, such as reliability, cooperation, delay, cost and ability of finishing a task, etc. The other part is the interactive trust. This value is the historical direct interaction record between the service requester and the backup device, which is produced after many interactions.

4.2.1 QoS trust

The method of calculating QoS trust is to evaluate the performance of the backup recovery device which can be expressed by several QoS attribute dimensions. There are multiple QoS attribute dimensions to be considered, and this paper only explains three typical dimensions which include service reliability $Q_R(s)$, delay $Q_D(s)$ and service cost $Q_C(s)$.

1. Service reliability

   The service reliability $Q_R(s)$ of the backup recovery device providing service s is the probability of correct response for the service request. That is, it is the probability that the service requester receives the desired results in the longest expected time. Service reliability is related with software and hardware configuration $Q_R^{con}(s)$ of the service provider p (backup recovery device). It is also related with the network connection metrics $Q_R^{net}(s)$ between the service requester r and the service provider p [23].

$$Q_R(s) = Q_R^{con}(s) + Q_R^{net}(s) \quad (7)$$

Author's personal copy

The calculation of $Q_R^{con}(s)$ is based on historical method, which is calculating the successful probability of a service. In formula (8), $N_{suc}(s)$ is the number of finishing s successfully in a period, and $N(s)$ is the scheduling number of the device.

$$Q_R^{con}(s) = N_{suc}(s)/N(s) \tag{8}$$

The network connection metrics $Q_R^{net}(s)$ is the reliability of a service routing between the service requester r and the service provider p.

$$Q_R^{net}(s) = 1 - \prod_{i=r}^{p}(1-\mu^i) = 1 - \prod_{i=r}^{p}(1-\mu_e^i)(1-\mu_d^i) \tag{9}$$

μ^i is the packet loss rate of each node i in the service routing from r to p. μ_e^i is the error rate of transmitting data packet of node i, μ_d^i is the packet drop rate of node i. There are many kinds of methods and tools to calculate these parameters, and we do not discuss more in this paper.

From the above formulas, we can obtain the service reliability $Q_R(s)$ of the backup recovery device providing service s.

$$Q_R(s) = Q_R^{con}(s) + Q_R^{net}(s) = N_{suc}(s)/N(s) + 1 - \prod_{i=r}^{p}(1-\mu_e^i)(1-\mu_d^i) \tag{10}$$

2. Delay

The delay $Q_D(s)$ of the backup recovery device providing service s is the time from device p receiving the request to the requester r receiving the service result. The delay $Q_D(s)$ is the sum of the mobile nodes' dealing delay and network transmission delay along the service path from p to r. The specific calculation method is as follows: suppose the mobile node's dealing delay is expressed as t_{dea}^i, and the transmission delay between two adjacent nodes on the network service path is expressed as $t_{tra}^{i,i+1}$. The delay $Q_D(s)$ of service s is expressed as formula (11).

$$Q_D(s) = \sum_{i=p}^{r-1}(t_{dea}^i + t_{tra}^{i,i+1}) + t_{dea}^r \tag{11}$$

In the practical application of formula (11), because the processing ability of current mobile nodes have been strengthened greatly, $t_{dea}^i = 0$ by default. For some computing services needing to be strengthened, such as video encoding or decoding, t_{dea}^ican be given by the service provider p, which is provided by the service description.

The network transmission delay is obtained from the sum of all the transmission delay between two adjacent nodes on the network service path. $t_{tra}^{i,i+1}$ satisfies formula (12).

$$t_{tra}^{i,i+1} = \alpha + \beta \cdot dist(i, i+1) \tag{12}$$

In formula (12), $dist(i, i+1)$ is Euclidean distance between two adjacent nodes, α and β are two factors [14].

3. Service cost

The service cost of s is the fee the service requester r needing to pay when using service s. This QoS parameter is given by service provider p who writes the cost into service description directly when registering service. Service discovery process takes the cost value of service s back.

Author's personal copy

4. Normalization

Suppose that there are m backup devices for a service s, and there are n QoS attributes to describe each device. This paper discusses three QoS attributes, therefore $n = 3$.

The QoS attributes set of the providers for service s can be written as $n * m$ matrix $A = (A_{ij}; 1 \le i \le n, 1 \le j \le m)$. Each row corresponds to a QoS attribute dimension, and each column corresponds to an attribute set for a service provider. Matrix A is expressed by formula (13).

$$A = \begin{pmatrix} Q_R(p_1) & Q_R(p_2) & \dots & Q_R(p_m) \\ Q_D(p_1) & Q_D(p_2) & \dots & Q_D(p_m) \\ Q_C(p_1) & Q_C(p_2) & \dots & Q_C(p_m) \end{pmatrix} \tag{13}$$

Through normalized matrix A, we can obtain matrix $B = (B_{ij}; 1 \le i \le n, 1 \le j \le m)$, which makes the values of matrix A more standard and easier to calculate [26]. The normalization process is as follows.

$$B_{ij} = \begin{cases} \frac{A_{ij} - A_j^{min}}{A_j^{max} - A_j^{min}} & if\ A_j^{max} - A_j^{min} \neq 0 \\ 1 & if\ A_j^{max} - A_j^{min} = 0 \end{cases} \tag{14}$$

$$B_{ij} = \begin{cases} \frac{A_j^{max} - A_{ij}}{A_j^{max} - A_j^{min}} & if\ A_j^{max} - A_j^{min} \neq 0 \\ 1 & if\ A_j^{max} - A_j^{min} = 0 \end{cases} \tag{15}$$

Formula (14) is used to handle the positive attribute value, such as service reliability. If the value is bigger, the service quality is higher. Formula (15) is used to deal with negative attribute value, such as delay and service cost. If the value is smaller, the service quality is better. A_j^{max} and A_j^{min} are the maximal and minimal attribute value in a row of matrix A. Matrix B is obtained from formula (14) and formula (15), and each element value of matrix B satisfies $0 \le B_{ij} \le 1$.

5. Weighted score

Formula (16) is used to calculate the QoS attribute weighted score for each backup device of service s. Based on each weighting factor $w_i (0 \le w_i \le 1, \sum_{i=1}^{n} w_i = 1)$, we can calculate each column of matrix B.

$$Score(p_j) = \sum_{i=1}^{n} w_i \cdot B_{ij}, \quad 1 \le j \le m \tag{16}$$

The service requester can express his preference by providing different weights w_i. For example, video transmission application requires high speed of data transmission, so the weight of delay is the biggest; important data request application requires high reliability, so the weight of service reliability is the biggest. From formula (16), we can get multiple scores of the backup devices, which will be used to compute direct trust degree.

4.2.2 Interactive trust

The direct trust degree is obtained from QoS trust and interactive trust. Except for QoS trust described in Section 4.2.1, the interactive trust between the requester r and the backup

Author's personal copy

recovery device p also need to be calculated. The interactive trust is the historical record of direct contact between r and p. The direct contact includes providing multimedia contents or transmitting data for each other, which is produced by multiple interaction and changes dynamically.

Suppose at time t_i, the number of successful interaction between r and p is $S_{r,p}$,the number of failed interaction is $F_{r,p}$, formula (17) shows the interactive trust between r and p [19].

$$T_{r,p} = \left(1 - \frac{1}{S_{r,p}+1}\right)\frac{S_{r,p}}{S_{r,p}+F_{r,p}} = \frac{(S_{r,p})^2}{(S_{r,p}+1)(S_{r,p}+F_{r,p})} \tag{17}$$

This paper uses formula (17) and does not use a linear function. Because with the increase of the successful interaction, the speed of this function close to 1 is very slowly. Therefore, it will cost more time for a node to increase trust to another node with formula (17).

4.2.3 Direct trust degree calculation

According to D-S evidence theory described in Section 4.1, this paper defines an identification frame or hypothesis space $\Theta = \{T, \sim T\}$, T means trust, and $\sim T$ means distrust. The power set of identification frame Θ is $P(\Theta)$, $P(\Theta) = \{\phi, \{T\}, \{\sim T\}, \{T, \sim T\}\}$, ϕ means null set.

The interactive trust $T_{r,p}$ obtained from Section 4.2.2 needs to correspond to the interactive trust vector V_{rp}, $V_{rp} = (m_{rp}(\{T\}), m_{rp}(\{\sim T\}), m_{rp}(\{T, \sim T\}))$. $m_{rp}(\{T\})$ means the probability of r trusting in p, $m_{rp}(\{\sim T\})$ means the probability of r distrusting in p. $m_{rp}(\{T, \sim T\})$ means the uncertainty probability of r trusting in p, and $m_{rp}(\{T\})+m_{rp}(\{\sim T\}) + m_{rp}(\{T, \sim T\}) = 1$. The three probability values can be expressed as x, y, z.

Suppose there is a mapping table of the QoS attribute weighted score and the provider trust vector. The weighted score explained in Section 4.2.1 needs to correspond to a device trust vector V_p, $V_p = (m_p(\{T\}), m_p(\{\sim T\}), m_p(\{T, \sim T\}))$, and $m_p(\{T\})+m_p(\{\sim T\})+ m_p(\{T, \sim T\}) = 1$, $m_p(\{T\})$ means the trust probability of service provider p, $m_p(\{\sim T\})$ means the distrust probability of p, $m_p(\{T, \sim T\})$ means the uncertainty probability of p. The three probability values can be expressed as x', y', z'. If the weighted score of p is higher, Belief function value $Bel(m_p(\{T\})) = x'$ is higher.

The direct trust degree of r to p is denoted by V_{dir} which changes with the variation of V_{rp} and V_p. In the beginning, there is no interaction between r and p, V_{dir} is only related with V_p and $V_{dir} = V_p(t_0) = (x'_0, y'_0, z'_0)$. When the service interrupts, we denote this time as t_i, and the direct trust of r to p is expressed as V_{dir} which satisfies formula (18).

$$V_{dir} = w \cdot V_{rp}(t_i) + (1 - w) \cdot V_p(t_i) \tag{18}$$

In formula (17), weighting factor w changes dynamically [24]. At time t_i, if$|x_i - x'_i| > |y_i - y'_i|$, the trust deviation is greater than the distrust deviation of two kinds of trust degrees (V_{rp} and V_p), so $w = w_1$. If $|x_i - x'_i| < |y_i - y'_i|$, the trust deviation is less than the distrust deviation, so $w = w_2$. If $|x_i - x'_i| = |y_i - y'_i|$, the trust deviation is equal to the distrust deviation, so $w = 0.5$. w_1 and w_2 satisfy $0 < w_2 < 0.5 < w_1 < 1$. The variation of w can punish the malicious nodes and prevent them from improving their trust values rapidly.

4.3 Recommended trust degree

The network is two layers structure based on cluster in this paper. Each cluster member evaluates its one hop neighbors and reports the evaluation results to its cluster head. The

Author's personal copy

cluster heads collect and calculate the trust evaluation of all the members in their clusters and update periodically. When the service requester r sends a request to the cluster head of p for the recommended trust degree, the cluster head sends the feedback to r. Formula (19) shows the recommended trust degree of p which is calculated and stored in the cluster head.

$$T_{rec}^{p} = avg_{i \in N}(T_i^p) = avg_{i \in N}(1 - p_{i,d}^{p})(1 - p_{i,t}^{p}) \tag{19}$$

In formula (19), N is the set of one hop neighbors of p. The neighbors observe and record the trust probability of abnormal behavior of p. In this paper, the abnormal behavior includes packet drop or tamper. Suppose $p_{i,d}^{p}$ is the packet drop rate of node i, $p_{i,t}^{p}$ is the packet tamper rate of node i. In order to obtain the recommended trust, the cluster head collects the trust evaluation of one hop neighbors of p and average the value.

The recommended trust T_{rec}^{p} needs to correspond to the recommended trust vector V_{rec}, $V_{rec} = (m_{rec}(\{T\}), m_{rec}(\{\sim T\}), m_{rec}(\{T, \sim T\}))$, $m_{rec}(\{T\})$ means the cluster head's recommended trust probability to p, $m_{rec}(\{\sim T\})$ means the cluster head's distrust probability to p, $m_{rec}(\{T, \sim T\})$ means the cluster head's uncertainty probability to p, and $m_{rec}(\{T\}) + m_{rec}(\{\sim T\}) + m_{rec}(\{T, \sim T\}) = 1$.

4.4 Trust degree combination

The core idea of D-S evidence theory is Dempster's combinational rule. The evidence information from different resources can be combined together to obtain a comprehensive result. According to the direct trust degree V_{dir} and recommended trust degrees V_{rec} obtained from Sections 4.2 and 4.3 respectively, we can use Dempster's combinational rule to calculate the comprehensive trust degree V of p, $V = (m(\{T\}), m(\{\sim T\}), m(\{T, \sim T\}))$.

Basic probability assignment (BPA) function of comprehensive trust T can be obtained based on formula (5).

$$\begin{aligned} m(\{T\}) &= m_{dir} \oplus m_{rec}(\{T\}) \\ &= \frac{1}{K} \cdot \sum_{A_1 \cap A_2 = \{T\}} m_{dir}(A_1) \cdot m_{rec}(A_2) \\ &= \frac{1}{K} \cdot m_{dir}(\{T\}) \cdot m_{rec}(\{T\}) \end{aligned} \tag{20}$$

Based on formula (2) and (20), Belief function (Bel) of comprehensive trust T can be expressed as formula (21).

$$Bel(\{T\}) = \sum_{B \subseteq \{T\}} m(B) = m(\{T\}) \tag{21}$$

The service requester can use formula (21) to calculate Bel value for every backup recovery device providing service s. The device with maximal Bel value will be selected to recover service s. So this is the service recovery method based on trust evaluation, and we will describe the algorithm for this method in detail.

5 Service recovery algorithm

The service recovery algorithm includes three process.

Service request process: when the service requester r needs some multimedia contents, he first sends a service request to the cluster head. The cluster head discovers if there are

Author's personal copy

required multimedia contents. If there are no such contents or not all the multimedia contents are in its cluster, the cluster head will send the service request to other cluster heads. This process is repeated until all the required multimedia contents are discovered. Then the data of multimedia contents will be sent to r.

Service interruption: a device providing service s may be failed to work which will cause service interruptions. Device failure includes several factors, such as malicious behavior, mobility and power limitation, etc.

Service recovery process: when the service interruption happens, compute the comprehensive trust degree V and Belief function (Bel) for backup recovery devices. This process is a circle. Choose the most reliable backup device to recover the service. Then construct service recovery routing and provide service for the service requester r continuously. The algorithm of this method can be illustrated in Fig. 3.

The pseudo code of service recovery algorithm is shown in Fig. 4.

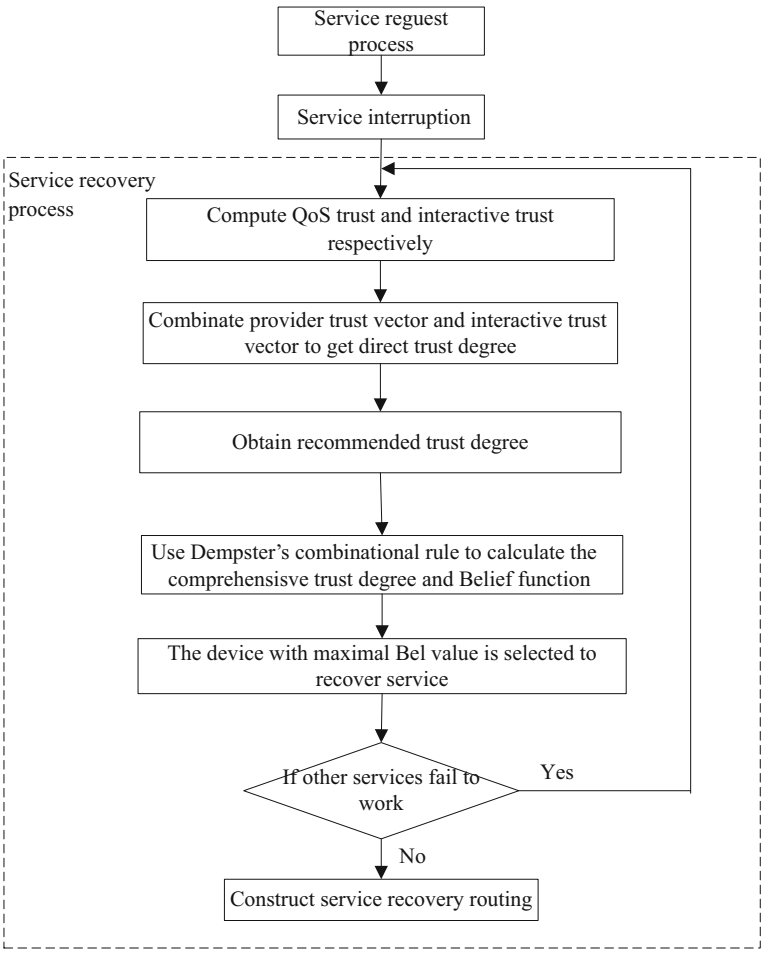


Fig. 3 Flowchart of service recovery algorithm

Author's personal copy

Begin
Input: requester p, required services $\{s_1, \cdots, s_n\}$, failed service s
While ($s \neq null$) do
$A \leftarrow Q_R(s), Q_D(s), Q_C(s)$ //calculate QoS trust, QoS attributes set of the providers for service s can be written as matrix A
$B \leftarrow A$ // normalize matrix A to matrix B
$Score \leftarrow B$ // calculate weighted scores of the backup devices
$V_{rp} \leftarrow T_{r,p}$ // interactive trust vector
$V_p \leftarrow Score$ // provider trust vector
$V_{dir} \leftarrow w \cdot V_{rp}(t_i) + (1-w) \cdot V_p(t_i)$ // direct trust degree
$V_{rec} \leftarrow T_{rec}^p$ //recommended trust vector
$Bel(\{T\}) \leftarrow m(\{T\})$ //calculate Belief function (*Bel*) of comprhensive trust T
select p with maximal *Bel*
return p
endwhile
End

Fig. 4 Pseudo code of algorithm

6 Simulation analysis

6.1 Simulation setup

In order to verify the performance of the method, this paper compares our service recovery method based on trust evaluation (SRMTE) with backup service replacement strategy(BSRS) [20], resend request strategy(RRS) [7], method with hybrid trust management model(HTMM) [1] and group-based trust management scheme (GTMS) [19]. BSRS and RRS are the service recovery methods without trust mechanism. HTMM and GTMS are the service recovery methods with trust mechanism. This paper conducts the simulation experiments and analyzes the performance of different methods respectively.

In our simulation experiments, $C++$ language is adopted to program in $VC++6.0$. The simulation environment and parameter settings are as follows: 100 nodes are distributed in the rectangle simulation area of $1500 \times 1500(m^2)$ and follow the random way mobility model (RWP) [12]. The maximal transmission radius of all the nodes is 300m. There are 10 types of services distributed in the nodes. Here service means providing multimedia content. For each service, there are 10 providers. Suppose all the nodes have been divided into clusters, and the number of clusters is 10. Each cluster contains 10 nodes. One node is cluster head, and the other 9 nodes are cluster members. Node max speed is from 2 m/s to 20 m/s. If a node moves for 5s, pauses for 3s and moves on. The time of executing a service is 5s. The number of concurrent requests to a node is 4. We use ad hoc on-demand distance vector routing (AODV) protocol. The simulation time is 600s. The service requesters are selected randomly in each simulation experiment which will produce multiple service requests.

6.2 Result analysis

This paper compares the simulation results of the five methods from two aspects including packet delivery ratio and service execution time.

Author's personal copy

1. Packet delivery ratio

Packet delivery ratio is the ratio of the number of successfully received packets to the number of packets sent per unit time, which is an important index of examining the service quality. The factors that affect packet delivery ratio are link interruptions caused by node movement or failure, transmission timeout and malicious nodes' discarding or tampering with the packet, etc. Suppose the number of requested services is 3 and 6 respectively, and the number of malicious nodes is 10. Figure 5 is the contrast figure of the packet delivery ratio of SRMTE, BSRS, RRS, HTMM and GTMS with the increase of the node max speed.

As can be seen from Fig. 5, regardless of the number of requested services is 3 or 6, the packet delivery ratio of the five methods decrease with the increase of the node max speed. When the node max speed is low, the packet delivery ratio is high. Because the nodes will not quickly move out of the transmission range of the service path, and the link is relatively stable and is not easy to be interrupted. With the increase of the node max speed, each method of packet delivery ratio gradually decreases. As the nodes move faster, the link is unstable, and the number of service interruptions increases. The frequency of discovering the backup nodes and repairing the service path is higher which reduces the packet delivery ratio.

Compared with the case of 3 requested services, the packet delivery ratio is lower when the number of the requested services increases to 6. If the number of requested services is small, the nodes needed to provide multimedia contents are less. The service is easier to finish and not prone to be interrupted, and the packet delivery ratio is higher. If the number of requested services increases, the nodes needed to finish the tasks also increase. The unstable factors of the links augment, and the possibility of service interruptions increases, which reduces the packet delivery ratio.

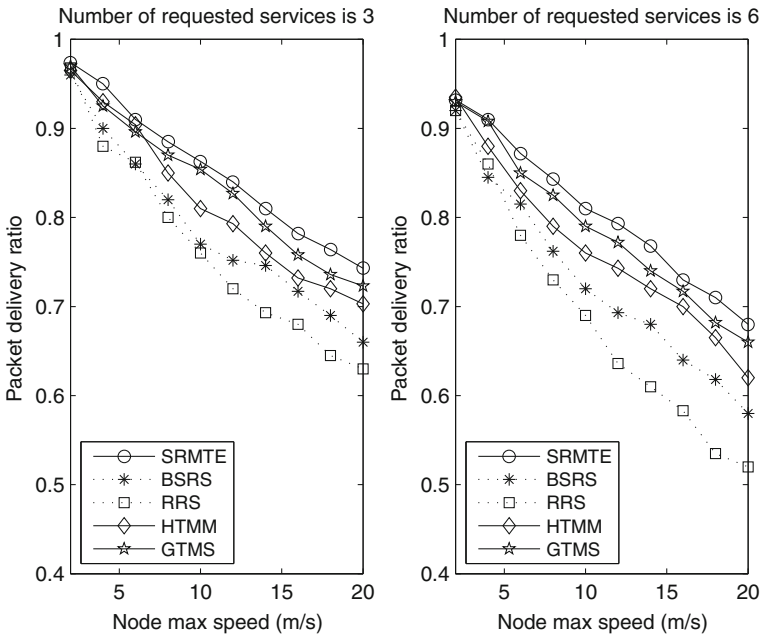


Fig. 5 Packet delivery ratio influenced by node max speed

Author's personal copy

Suppose the number of requested services is 3 and 6 respectively, and the node max speed is 10 m/s. Figure 6 is the contrast figures of the packet delivery ratio of SRMTE, BSRS, RRS, HTMM and GTMS with the increase of the number of malicious nodes.

As can be seen from Fig. 6, the packet delivery ratio of these five methods decreases with the increase of the number of malicious nodes. If the number of malicious nodes is small, the packet delivery ratio is not significantly affected. When the number of malicious nodes exceeds a certain percentage, such as 20 %, namely 20 in our experiment, the decreasing speed of packet delivery ratio becomes apparent, especially the two methods (BSRS and RRS). When the number of malicious nodes is 40, the packet delivery ratio of BSRS and RRS drops below 0.5 or 0.4 in Fig. 6. This is because BSRS and RRS do not adopt trust mechanism and are strongly influenced by malicious nodes. In the other three methods (SRMTE, HTMM and GTMS) with trust mechanism, the decreasing speed of the packet delivery ratio of SRMTE is the slowest.

Compared with the case of 3 requested services, the packet delivery ratio decreases quickly when the number of the requested services increases to 6. If the number of requested services increases, the nodes including malicious nodes needed to provide multimedia contents also increase which result in the reduction of the packet delivery ratio.

Figures 5 and 6 illustrate that the packet delivery ratio of the three methods (SRMTE, HTMM and GTMS) with trust mechanism is higher than the two methods (BSRS and RRS) without trust mechanism. Compared with other methods, the packet delivery ratio of SRMTE is the highest.

2. Service execution time

Service execution time, including the time of service interruptions and recovery is a period from the requester sends a request to receive all the service results successfully.

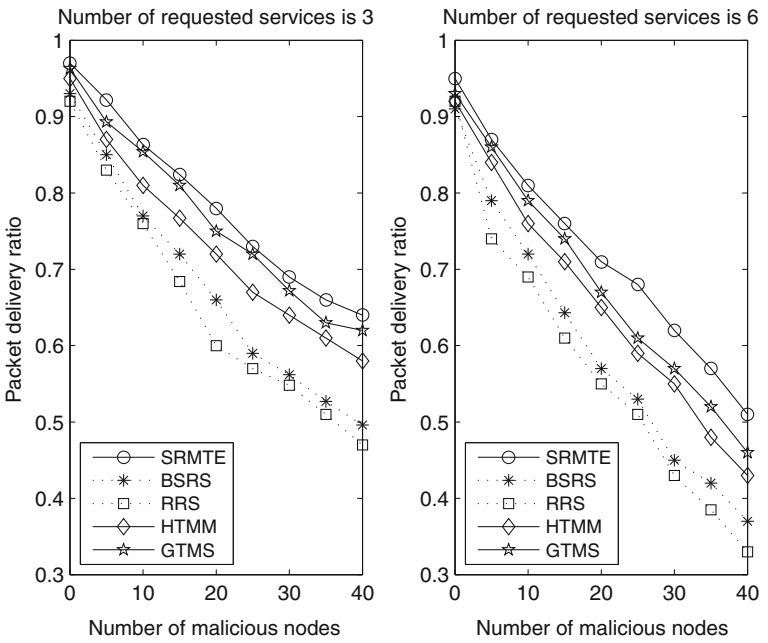


Fig. 6 Packet delivery ratio influenced by number of malicious nodes

Author's personal copy

Suppose the number of requested services is 3 and 6 respectively, and the number of malicious nodes is 10. Figure 7 is the contrast figure of the service execution time of SRMTE, BSRS, RRS, HTMM and GTMS with the increase of the node max speed.

Figure 7 shows that the service execution time of the five methods reduces with the increase of the node max speed. Because it is easier and faster to discover the needed nodes providing multimedia contents within the transmission range. Compared with the case of 3 requested services, the service execution time is longer when the number of the requested services increases to 6. If the number of requested services is bigger, the nodes needed to provide multimedia contents increase. The recovery time for service interruptions also increase which will extend the service execution time.

Suppose the number of requested services is 3 and 6 respectively, and the node max speed is 10 m/s. Figure 8 is the contrast figures of the service execution time of SRMTE, BSRS, RRS, HTMM and GTMS with the increase of the number of malicious nodes.

Figure 8 illustrates that the service execution time of the five methods increase with the increase of the number of malicious nodes. When the number of malicious nodes is zero in the beginning, the service execution time of all the methods is not affected and relatively short. With the increase of the number of malicious nodes, the impact on the service execution gradually augments, and the consumption time also increases. BSRS and RRS have no trust mechanism and cannot reduce the impact of malicious nodes. When the number of malicious nodes exceeds a certain percentage, the service execution time of these two methods increases quickly, and the service execution time of SRMTE, HTMM and GTMS increases slowly. Compared with the case of 3 requested services, the service execution time is longer when the number of the requested services increases to 6. If the number of requested services increases, the nodes including

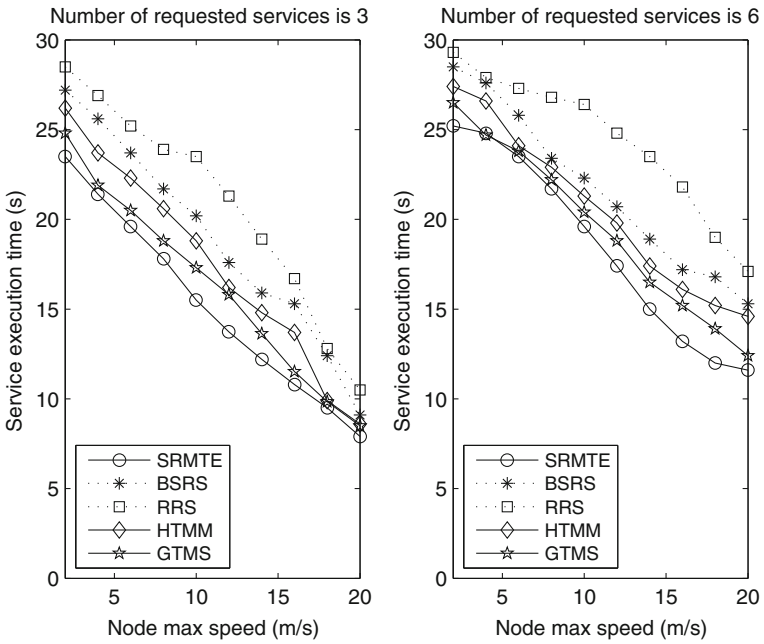


Fig. 7 Service execution time influenced by node max speed

Author's personal copy

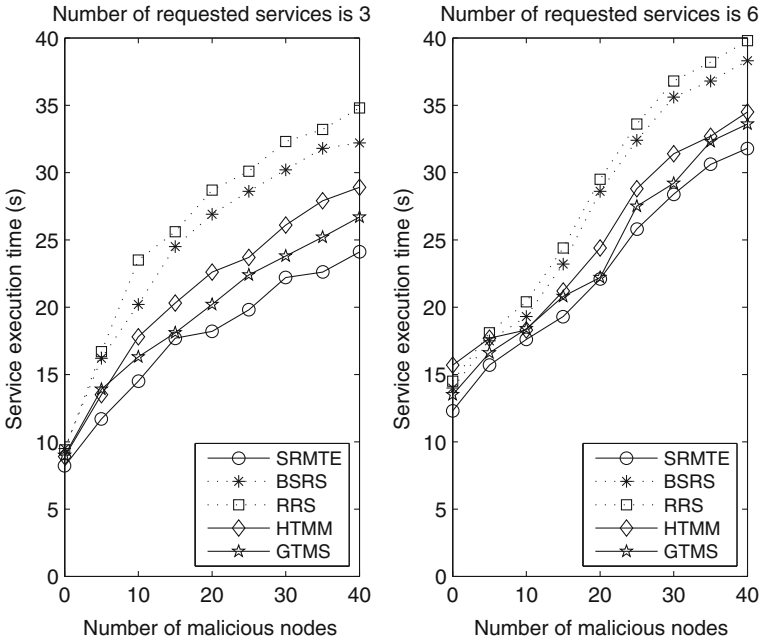


Fig. 8 Service execution time influenced by number of malicious nodes

malicious nodes needed to provide multimedia contents also increase which result in costing more time to execute services.

In the simulation experiments, we consider another case. The number of clusters gradually increases from 4 to 20, but each cluster still contains 10 nodes. One node is cluster head, and the other 9 nodes are cluster members. There are 10 types of services distributed in the nodes, and the number of nodes for each service is equal. Other conditions are the same as Section 6.1. Suppose the number of requested services is 6, the node max speed is 10 m/s, the number of malicious nodes accounts for 10 % of all the nodes. Figure 9 is the contrast figure of the packet delivery ratio and the service execution time of SRMTE, BSRS, RRS, HTMM and GTMS with the increase of the number of clusters.

When the number of clusters is not more than 12, the packet delivery ratio of these five methods increases rapidly. If the number of clusters is less, the efficiency of service discovery and recovery is lower, which causes the packet delivery ratio lower. When the number of clusters begins to increase, the service resources of each node become densely distributed within the region. The communication among cluster heads is faster and more convenient. The efficiency of service discovery and recovery is enhanced, which causes the packet delivery ratio increasing. When the number of clusters is more than 12, the packet delivery ratio slightly increases or maintains at a stable value. Because the distribution of the clusters and services is symmetrical and dense, it is very easy to find all kinds of services. The influence of cluster increase to the packet delivery ratio is very small.

When the number of clusters is small, the links between nodes are easy to interrupt, and the service execution time is longer. With the increase of the number of clusters, the service execution time of five methods decreases gradually. Because the links between nodes also increase, the service requester is able to discover required services quickly. When the

Author's personal copy

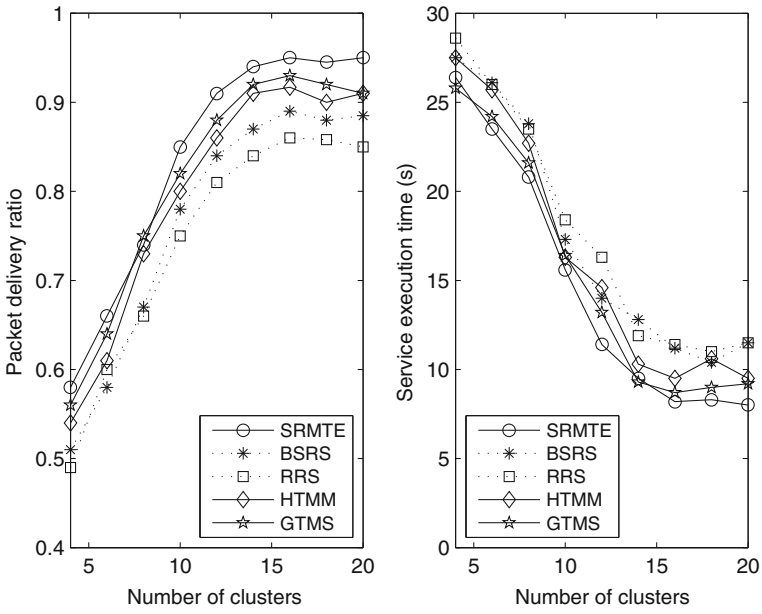


Fig. 9 Service quality influenced by number of clusters

number of clusters is more than 14, the situation of various link interruptions is very little. The service execution time of each method is maintained at a stable value, and the cluster increase has very little influence to the service execution time.

In summary, compared with the two methods (BSRS and RRS) without trust mechanism, the packet delivery ratio of the three methods (SRMTE, HTMM and GTMS) with trust mechanism is higher, and the service execution time is shorter. In BSRS, if a node providing service fails, the strategy sorts the available backup nodes with an algorithm. The backup node with the highest priority will be selected to replace the failed node. In RRS, if the service interrupts, the service requester will resend a request and reconstruct a service path. This method involves more nodes, consumes more time and greatly affects the packet delivery ratio whose performance is worse than BSRS.

In HTMM, the trust relation evaluation between nodes need too many evidence including the local storage information of node, the valid certificate, the third part's recommendation trust evaluation and the behavior trust evaluation from the monitoring node. The evidence collection and calculation process are complicated. In GTMS, all the sensor nodes and the cluster heads evaluate others periodically and report the results to their superiors. It will greatly cost the nodes and network resources, especially for the sensor nodes whose power, memory and computation ability are very limited. Compared with these two methods, the packet delivery ratio of SRMTE is higher, and the service execution time is shorter. The performance of SRMTE is better than others.

7 Conclusions

Mobile social network is vulnerable to malicious or selfish nodes. In order to reduce the harm of these nodes and ensure users' service experience of sharing multimedia contents,

Author's personal copy

this paper presents a service recovery method based on trust evaluation. The users are divided into multiple tourism groups according to their interests and geographic location in this paper. They share multimedia contents including geographic location, text, pictures, music and video with the mobile devices.

Some nodes have malicious behavior, such as discarding or tampering with packet. These factors will cause service interruptions in the process of providing multimedia contents for the user. When the service interruption happens, how to choose the more reliable backup device, reduce interruption number and improve the user's experience of sharing multimedia contents is the object of the paper. In this paper, we propose a trust degree evaluation method based on D-S evidence theory. The requester calculates the direct trust degree according to the QoS trust and interactive trust of the backup device and obtains the recommended trust degree from the cluster head, then uses the evidence combination rule to calculate the comprehensive trust degree of the backup devices. The backup device with the highest trust value will be selected to recover the service. We compare SRMTE with other methods through simulation experiments.

The simulation results show that with the increase of the node max speed and the number of malicious nodes or clusters, the proposed method SRMTE can effectively improve the packet delivery ratio and reduce the service execution time. Because the method adopts the clustering network structure. When a user needs some multimedia contents, he conducts service discovery and recovery through multiple cluster heads. According to the clustering network, we propose a service recovery method based on trust evaluation which adopts D-S evidence theory. When the resources on a device is limited, the clustering network structure can maximize the packet delivery ratio, reduce the link interruptions and service execution time and accelerate the service recovery. Of course, the number of clusters should be a reasonable value. Too many clusters will increase the network consumption, and too little clusters will reduce the efficiency of service discovery and recovery. In conclusion, this method is favorable for users to share multimedia contents quickly and conveniently.

In the next stage, aiming at multimedia application scenario, such as video conference in mobile social network, how to improve the transmission efficiency for the data sensitive to time and ensure users' smooth and stable service experience is our object. We will study and design the detection mechanism of abnormal device nodes. Before invoking nodes to provide multimedia contents, the mechanism excludes the malicious nodes in advance. In order to ensure the normal video play in the receiving node, we will adopt the information feedback mechanism to adjust the data transmission rate of the node providing multimedia contents.

Acknowledgments The work is supported by National Natural Science Foundation of China (61302078, 61372108, 61370220), Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant (15IRTSTHN010).

References

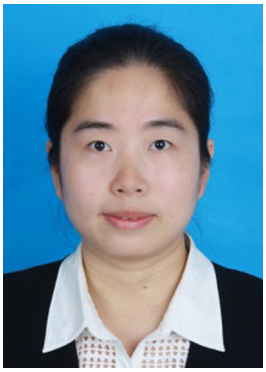
1. Aivaloglou E, Gritzalis S (2010) Hybrid trust and reputation management for sensor networks. Wirel Netw 16(5):1493–1510. doi:10.1007/s11276-009-0216-8
2. Amgoth T, Jana PK (2014) Energy efficient and load balanced clustering algorithms for wireless sensor networks. Int J Inf Commun Technol 6(3–4):272–291. doi:10.1504/IJICT.2014.063216
3. Bao FY, Chen IR, Chang MJ, Cho JH (2012) Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans Netw Serv Manag 9(2):169–183. doi:10.1109/TCOMM.2012.031912.110179

Author's personal copy

4. Batra PK, Kant K (2016) LEACH-MAC: a new cluster head selection algorithm for wireless sensor networks. Wirel Netw 22(1):49–60. doi:10.1007/s11276-015-0951-y
5. Bellavista P, Montanari R, Das SK (2013) Mobile social networking middleware: a survey. Pervasive Mob Comput 9(4):437–453. doi:10.1016/j.pmcj.2013.03.001
6. Boix EG, Carreton AL, Scholliers C, Van Cutsem T, De Meuter W, D'Hondt T (2011) Flocks: enabling dynamic group interactions in mobile social networking applications. In: 26th annual ACM symposium on applied computing, pp 425–432. doi:10.1145/1982185.1982277
7. Chen WY, He ZY, Ren G, Sun WW (2008) Service recovery for composite service in MANETs. In: Proceeding of IEEE international conference on wireless communication, networking and mobile computing, pp 1–4. doi:10.1109/WiCom.2008.630
8. Chen WY, Xu YX, Peng B, Sun WW (2008) Dynamic monitor based service recovery for composite service in MANETs. In: Proceeding of 11th IEEE international conference on communication technology, pp 557–560. doi:10.1109/ICCT.2008.4716120
9. Dempster A (1967) Upper and lower probabilities induced by multi-valued mapping. Ann Math Stat 38:325–339
10. Dooms S, De Pessemier T, Verslype D, Nelis J, De Meulenaere J, Van den Broeck W, Martens L, Develder C (2014) OMUS: an optimized multimedia service for the home environment. Multimedia Tools Appl 72(1):281–311. doi:10.1007/s11042-012-1347-y
11. Hu R, Liu JX, Liu XF (2011) A trustworthiness fusion model for service cloud platform based on D-S evidence theory. In: 11th IEEE/ACM international symposium on cluster, cloud and grid computing, pp 566–571. doi:10.1109/CCGrid.2011.31
12. Johnson DB, Maltz DA (1996) Dynamic source routing in ad hoc wireless networks. Mobile Comput 353:153–181
13. Li L, Wang Y (2009) Trust evaluation in composite services selection and discovery. In: 2009 IEEE international conference on services computing, pp 482–485. doi:10.1109/SCC.2009.70
14. Li X, Qian ZZ, You I, Lu SL (2014) Towards cost efficient mobile service and information management in ubiquitous environment with cloud resource scheduling. Int J Inf Manag 34(3):319–328. doi:10.1016/j.ijinfomgt.2013.11.007
15. Maria Kalavathy G, Edison Rathinam N, Seethalakshmi P (2012) Self-adaptable media service architecture for guaranteeing reliable multimedia services. Multimedia Tools Appl 57(3):633–650. doi:10.1007/s11042-010-0664-2
16. Paul A, Rho S, Bharnitharan K (2014) Interactive scheduling for mobile multimedia service in M2M environment. Multimedia Tools Appl 71(1):235–246. doi:10.1007/s11042-013-1490-0
17. Ruocco M, Ramampiaro H (2014) A scalable algorithm for extraction and clustering of event-related pictures. Multimedia Tools Appl 70(1):55–88. doi:10.1007/s11042-012-1087-z
18. Shafer G (1976) A mathematical theory of evidence. Princeton University Press, New York
19. Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song YJ (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712. doi:10.1109/TPDS.2008.258
20. Sun LL, An JW, Yang Y, Zeng M (2011) Recovery strategies for service composition in dynamic network. In: 2011 International conference on cloud and service computing, pp 60–64. doi:10.1109/CSC.2011.6138553
21. Wang Y, Dai GP, Hou YR (2009) Dynamic methods of trust-aware composite service selection. Chin J Comput 32(8):1668–1675. doi:10.3724/ SP.J.1016.2009.01668
22. Xia H, Jia ZP, Li X, Ju L, Sha EHM (2013) Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw 11(7):2096–2114. doi:10.1016/j.adhoc.2012.02.009
23. Yang K, Galis A, Chen HH (2010) QoS-aware service selection algorithms for pervasive service composition in mobile wireless environments. Mobile Netw Appl 15:488–501. doi:10.1007/s11036-009-0189-y
24. Yang K, Ma JF, Yang C (2011) Trusted routing based on D-S evidence theory in wireless mesh network. J Commun 32(5):89–103
25. Yang ZM, Zhang BY, Dai JP, Champion AC, Xuan D, Li D (2010) E-SmallTalker: a distributed mobile system for social networking in physical proximity. In: 2010 International conference on distributed computing systems, pp 468–477. doi:10.1109/ICDCS.2010.56
26. Zeng LZ, Benatallah B, Ngu AHH, Dumas M, Kalagnanam J, Chang H (2004) QoS-aware middleware for web services composition. IEEE Trans Softw Eng 30(5):311–327
27. Zhang ZY (2012) Frontier and methodologies on digital rights management for multimedia social networks. Int J Digital Content Technol Appl 6:245–249. doi:10.4156/jdcta.vol6.issue9.31
28. Zhang ZY, Wang KL (2013) A trust model for multimedia social networks. Soc Netw Anal Min 3(4):969–979. doi:10.1007/s13278-012-0078-4

Author's personal copy

29. Zhang K, Liang XH, Shen XM, Lu RX (2014) Exploiting multimedia services in mobile social networks from security and privacy perspectives. IEEE Commun Mag 52(3):58–65. doi:10.1109/MCOM.2014.6766086



Danmei Niu a Ph.D candidate at State Key Laboratory of Networking and Switching Technology at Beijing University of Posts and Telecommunications. She received the Masters degree from Henan University of Science and Technology in 2006. Her research interests include pervasive communication network, device and network management.

Lanlan Rui associate professor at State Key Laboratory of Networking and Switching Technology at Beijing University of Posts and Telecommunications. She received a PhD in Computer Science from Beijing University of Posts and Telecommunications in 2010. Her interests include pervasive communication network, network management, quality of service (QoS) and self-managing systems.

Author's personal copy

Haoqiu Huang a Ph.D. candidate from State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications (BUPT), Beijing, China. He received his M.Sc. (2012) from Shenyang Ligong University. His main research interests include architect ures and protocols design and optimization for wireless ad hoc networks, information-centric networking for the future Internet.

Xuesong Qiu received the Ph.D degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2000. He is a Professor and Ph.D supervisor. He published about 100 SCI/EI index papers. Professor Qiu has got 13 national and provincial scientific and technical awards, including the national scientific and technical awards (second-class) twice.