The Computer Journal Advance Access published October 4, 2014

doi:10.1093/comjnl/bxu091

A Trust Routing for Multimedia Social Networks

Guowei Wu[1], Zuosong Liu[1], Lin Yao[1,*], Jing Deng[2] and Jie Wang[1]

[1]*School of Software, Dalian University of Technology, Dalian 116023, China*
[2]*Department of Computer Science, University of North Carolina at Greensboro, Greensboro, USA*
**Corresponding author: yaolin@dlut.edu.cn*

Due to the disconnected and store-and-forward architecture in multimedia social networks (MSNs), routing becomes a great challenge with the frequent path disruptions. Moreover, some nodes in MSNs tend to be selfish or malicious, e.g. they sometimes will not forward packets for other nodes or will launch passive and active attacks in order to save their limited resources such as bandwidth, battery or storage. In order to address this issue, we propose a fuzzy-based trust management technique for context-based routing in MSNs. We incorporate social trust metrics and quality of service metrics into our trust model. By adopting fuzzy sets, every node can evaluate the credibility of other nodes based on the direct and indirect relationship. By ranking all its neighbors according to the trust values, each node can purge untrustworthy nodes. Since only trusted nodes' packets will be forwarded, the selfish or malicious nodes have the incentive to behave well again in order to be able to send packets. Additionally, we perform extensive security and performance evaluation with the opportunistic network environment simulator. The simulation results show that our trust model can dynamically update the trust value in real time, effectively measure the trust relationship and correctly identify malicious or selfish nodes. Furthermore, the proposed trust routing is a lightweight protocol balancing the message overhead and delivery ratio.

Keywords: trust model; fuzzy sets; multimedia social network; context-based routing

Received 14 September 2013; revised 17 July 2014
Handling editor: Zhiyong Zhang

1. INTRODUCTION

The rapid development of network socialization has led to the emergence of different services and functions provided by multimedia social networks (MSNs). These MSNs offer network services, and copyrighted digital contents (e.g. images and videos) that are shared among nodes within social networks anytime and anywhere [1]. More portable and affordable mobile devices have made MSNs rather popular. In such networks, people move around and contact others based on their social connections such as workplace, friendship and interest [2]. MSNs demonstrate several unique features: dynamic topology, high mobility, episodic connectivity and a store-and-forward architecture. Due to the frequent path disruptions, routing for MSNs has become a great challenge.

Epidemic [3] has been proposed as a routing approach in sparse and/or highly mobile networks. Epidemic routing is able to achieve minimum delivery delay at the expense of consuming more resources such as buffer space, bandwidth and transmission power. More recently, context-based routing schemes have been proposed for the opportunistic networks and have been demonstrated to be more efficient and accurate [4, 5]. Context information represents user behavior and interaction history such as current working environment, locations and prior rendezvous with other nodes.[1] Such information can be used to help with forwarder selection.

Selfish and malicious nodes in MSNs cause another challenge in the routing. Routing in MSNs relies on cooperation among participating nodes. However, cooperative forwarding incurs costs to forwarding nodes, both in terms of battery power and storage, which are usually constrained in mobile devices. Hence, selfish nodes may refuse to forward messages for other nodes, counteracting the cooperative effort for the entire network. Additionally, malicious attackers may launch deny of service (DoS) attacks based on flooding, consuming limited caches as well as communication bandwidth. Thus, an efficient routing protocol must be able to

[1]In this paper, we use the terms 'user' and 'node' interchangeably.

protect itself from selfish and malicious attacks. Unfortunately, such a problem has either been ignored [4–6] or addressed by a technique that requires a centralized unit or a trusted third-party [7–12].

In this paper, we propose a trust routing scheme to create incentives and stimulate the cooperation among nodes. Every node forwards messages based on its trust relationship with others. In our trust model, a node's credibility is computed by combining social trust measurements with some quality of service (QoS) requirements. Social trust measurements include the probability of successful interactions and the feedback of digital content. QoS trust measurements refer to context matching ratio and energy. In this paper, fuzzy sets are used to evaluate the trustworthiness with imprecise information in a non-probabilistic environment. By ranking all neighbors based on their trust values, each node only forwards packets to those with higher trust values.

Our contributions of this work are as follows.

(i) Different from other works [13, 14], our trust model does not assume Poisson distribution for the node behaviors.
(ii) Combining social attributes and QoS requirements, every node can adopt fuzzy sets to calculate the trust values dynamically. On the other hand, the trust values are calculated based on the predefined metrics and/or deterministic values in most other trust models [6, 9, 15].
(iii) We further design a recovery and mobile firewall mechanism to prevent the spread of viral content and balance the energy consumption.

The rest of the paper is organized as follows. In Section 2, we briefly introduce fuzzy sets and context-based routing. In Section 3, we provide a brief introduction to the network model, attack model and some security requirements. We present the details of our proposed scheme in Section 4. The simulation results are discussed in Section 5. In Section 6, we describe the related work. Finally, we conclude our work in Section 7.

2. PRELIMINARIES

In this section, we briefly introduce fuzzy sets and context-based routing.

2.1. Fuzzy sets

Different from the classical set theory in which the membership of elements is assessed in binary terms: an element either belongs or does not belong to a set. A fuzzy set is defined by a membership function which maps the domain of interest into the interval [0, 1]. Let X be a space of points, $X = \{x\}$. A fuzzy set A is defined by a membership function $f_A(x)$, which associates each point in space X to a real number in [0, 1] and the value of $f_A(x)$ represents the grade of membership of x in the set A [16]. The closer the value is to 1, the higher the grade of membership is.

For a finite set $U = \{u_1, u_2, \ldots, u_m\}$, the membership vector is calculated:

$$V = \{f_A(u_1), f_A(u_2), \ldots, f_A(u_m)\}. \quad (1)$$

Considering different vector elements may have different roles, we define $\{w_1, w_2, \ldots, w_i, \ldots, w_m\}$ as the weight vector. Then, the final judgment value is calculated:

$$v_A = \sum_{i=1}^{m} w_i \times f_A(u_i). \quad (2)$$

Similarly, $f_B(x)$ represents the grade of membership of x in the set B and its final value v_B is calculated. Then, we define $V' = \{v_A, v_B, \ldots, v_X\}$ to represent the grade of membership of x. Based on the maximum degree of membership, each element in the set U belongs to the set $v_i = \max(V')$.

Fuzzy sets have been commonly used with imprecise information in a non-probabilistic sense, such as artificial intelligence and control engineering. Works in [17–19] adopt fuzzy sets to evaluate the trustworthiness and deal with the uncertain trust information coming from other nodes.

2.2. Context-based routing

In some mobile networks such as MSNs, it is sometimes difficult to establish a complete path from source to destination. Thus, the conventional wireless routing protocols cannot be applied. In order to improve network performance, routing protocols in MSNs need to achieve reliability even with frequent link disconnection. Flooding-based routing protocols can solve this problem, but only with excessive overhead and energy consumption. It is unsuitable for the portable devices with limited resources. Context information in these networks can be exploited to improve routing performance, by helping with routing decisions.

In this section, we briefly introduce an original design of an epidemic forwarding protocol where heuristic is based on the context (e.g. workplace, hobbies, personal information, etc.) [5]. The idea behind context-based routing protocol is that the chance of encounter is higher when two users share more social contexts.

We assume that there are N nodes. The context of a node n_i is defined as a set of attributes A_{ij}. Here A_{ij} consists of an attribute name E_i and its value V_{ij}. E_i is known by all nodes. As shown in Fig. 1, there are four nodes and three attributes (E_1 = workplace, E_2 = status, E_3 = mail). When the source n_s sends a message M to the destination n_d, n_s must first add some context information of n_d into the message header. For example, when n_1 invites n_3 to join a party, n_1 will broadcast

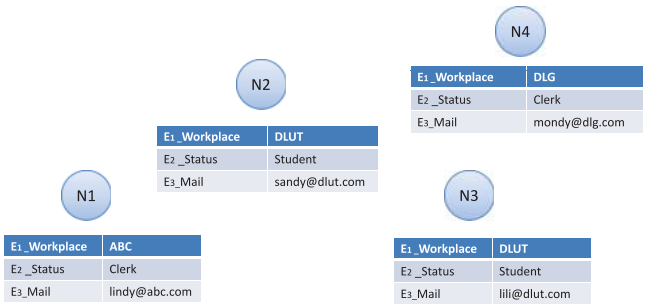

FIGURE 1. Context-based routing.

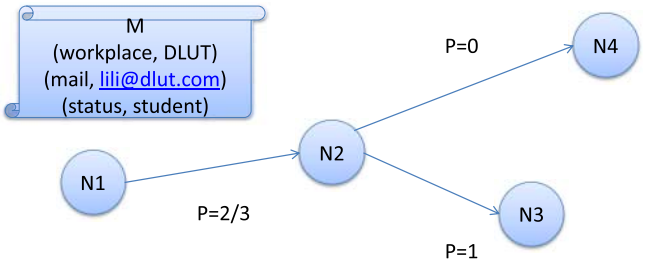

FIGURE 2. A communication scenario.

M with the payload 'Join us in the party tonight at 10 pm.' and the header message '(workplace, DLUT), (status, student), (mail, lili@dlut.com)'. When n_1 meets n_2, n_1 will compute the matching ratio $P = \frac{2}{3}$, which shows that n_2 has more chances to meet n_3. Then n_1 will forward M to n_2 (Fig. 2).

3. NETWORK MODEL AND SECURITY REQUIREMENTS

In this section, we introduce the network model, attack model and some security requirements.

A. *Network model*

Our trust routing protocol uses several specific types of context information, on which a node credibility is evaluated. As shown in Fig. 3, each node is given one profile to represent its identification and its context information [5], such as '(workplace, DLUT), (mail, lili@dlut.com), (status, student)'. Based on different profiles, an MSN can be divided into multiple social cliques. When n_s sends a message M to n_d, n_s will first add n_d's context information into its message header. Every encounter will compare this header with its own profile to decide whether to forward the message. Moreover, our scheme is based on the following assumptions [5, 8]:

(i) Every node uses omni-directional transceivers to monitor its neighbors in promiscuous mode.

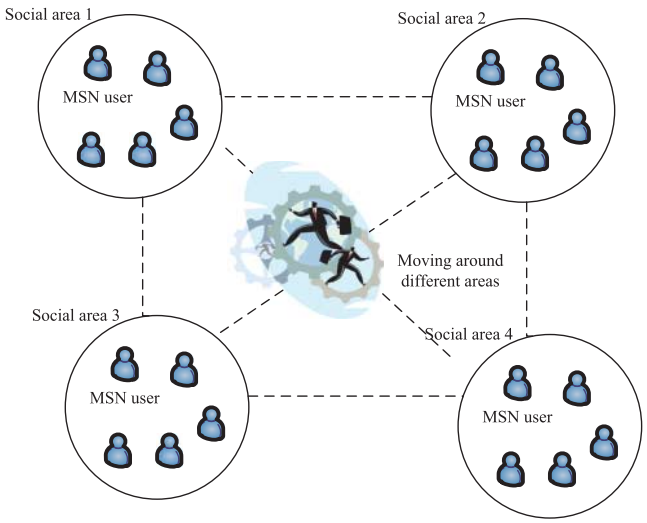

FIGURE 3. System model.

(ii) All links are bi-directional and all nodes have the same transmission range. A packet will be received/overheard by nodes within the transmission range.

B. *Attack model*

Usually, network attackers are categorized into passive and active ones.

(i) Passive attackers: these passive attackers track messages by monitoring the wireless links.
(ii) Active attackers: these active attackers can corrupt messages and/or launch DoS attacks.

Obviously, active attackers are stronger than passive attackers. When nodes share and exchange multimedia content as well as other content, active attackers (malicious nodes) try to break the basic routing functionality by dropping packets, injecting faked data or malicious codes, etc. Passive attackers (selfish nodes) only try to save their limited resources by dropping packets.

In this paper, we mainly focus on the behavior of passive attackers (selfish nodes) with dropping packets.

C. *Security requirements*

In order to mitigate security threats, trust has been introduced from sociology to evaluate node credibility through sharing history and other potential behavior records [20]. A success trust relationship should be able to satisfy the following security requirements:

(i) A message carrier can distinguish selfish and normal nodes. It only forwards packets to normal nodes or trusted nodes but not to those selfish users.

(ii) An attacker can be distinguished by a normal node even though it does not have direct interaction with the normal node.
(iii) After detecting selfish or malicious nodes, normal nodes punish them by refusing to forward messages from them.
(iv) An attacker cannot share faked content with other nodes.

4. CONTEXT-BASED FUZZY TRUST ROUTING PROTOCOL

In this section, we will elaborate our context-based Fuzzy Trust routing protocol. The trust model is used to provide valuable trust evaluation of every entity and to facilitate safe and effective interaction among nodes. Nodes share and transmit digital content based on a certain trust relationship. In order to accurately evaluate trust relationship among nodes and choose the best forwarding nodes, our scheme has three stages: trust factor observation, trust calculation and routing decision, shown in Fig. 4. Furthermore, we introduce the recovery and mobile firewall mechanism to prevent the spread of viral content. In Table 1, the frequently used notations are listed.

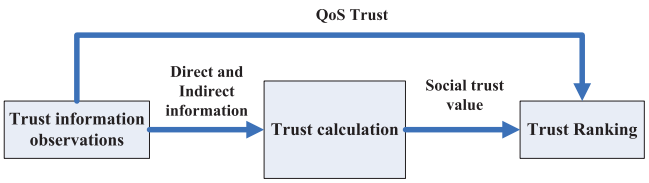

FIGURE 4. Trust model framework.

TABLE 1. Notations and variables.

Symbols	Meaning
n_i	Node i
FT_{ij}	n_i's direct trust value on n_j
ST_{ij}	n_i's indirect trust value on n_j
Psi_{ij}	The probability of successful interactions between n_i and n_j
P_{ij}	The context matching ratio between n_i and n_j
E_{ij}	The energy of n_j detected by n_i
Fed_{ij}	n_i's credible feedback of digital content on n_j
Ns_{ij}	The total number of packets that n_i has sent to n_j
Nf_{ji}	The total number of packets that n_j has forwarded for n_i
$RTA_{i\to j}$	The trust similarity between n_i and n_j
$Prof(i)$	The context information of n_i
Vso_{ij}	n_i's social trust value on n_j
$Vfin_{ij}$	n_i's final trust value on n_j

4.1. Trust factor observation

We distinguish two kinds of trust decision factors: direct trust and indirect trust information. The direct trust information is generated from physical neighbors and the indirect trust information is derived from the recommendation of such neighbors.

Direct trust relationship can be obtained from the evidence created by the physical interactions. The evaluating entity conducts a trust evaluation on the target entity based on its own experiences. For example, n_i determines the trust level of n_j solely based on n_i's direct experiences with n_j (see Fig. 5). In our system, we use fuzzy theory to describe the direct trust model.

Indirect trust relationship can be obtained from the propagation of direct trust information. In MSNs, it is unlikely for one node to share digital content with each of the nodes. Thus, recommended trust becomes the only means to evaluate nodes without direct interactions. For example, n_i has a direct interaction with n_j and n_j has a direct interaction with n_k. When n_j forwards the direct trust value of n_k to n_i, n_i can establish a new indirect trust relationship with n_k based on these second-hand trust evidence.

To evaluate the trust relationship, we combine social and QoS metrics.

(i) Social trust: The probability of successful interactions and the credible feedback of digital content are used as the social trust metrics to judge whether the node is malicious or not.

The probability of successful interactions: This probability is used to collect information about the packet forwarding behaviors of the neighbors [17]. Every node, such as n_i, maintains two records for its neighbor n_j, Ns_{ij} (the total number of packets sent from n_i to n_j) and Nf_{ji} (the total number of packets forwarded for n_i by n_j). The probability of successful interactions between n_i and n_j,

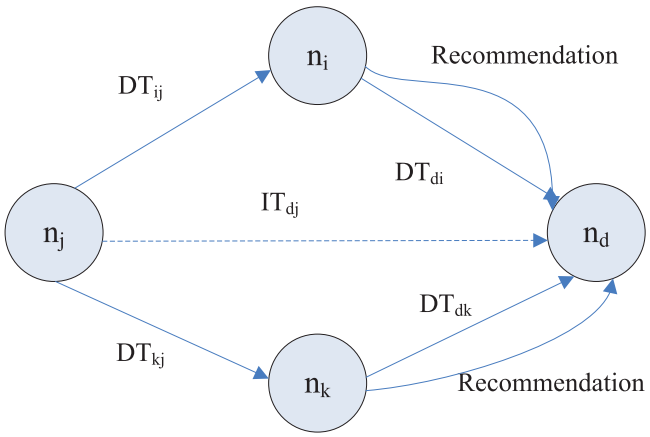

FIGURE 5. Trust relationship.

Psi_{ij}, evaluating whether n_j is honest enough to forward packets for n_i, can be calculated as follows:

$$Psi_{ij} = \frac{Nf_{ji}}{Nf_{ji} + \lambda(Ns_{ij} - Nf_{ji})}. \quad (3)$$

Here λ is the penalty weight for the selfish node's behavior, with a bigger λ representing a higher penalty.

The credible feedback of digital content: In MSNs, digital content sharing is one of the most important functions. Once a node receives digital content, it can provide a feedback based on the safe credibility of the shared digital content. Thus, the creditable feedback of digital content Fed_{ij} can be used as one social trust metric [12]. The value is in [0, 1], where 1 means that the shared digital content is deemed safe and 0 means the content is not credible or safe.

(ii) QoS trust: QoS trust is to evaluate the capability of delivering messages to the destination. The context matching ratio and energy are used to measure the QoS trust level.

The context matching ratio: We assume that every node has a context profile. More shared context may provide more encounter chances. In our paper, the context matching ratio P_{dj} is calculated in the following equation:

$$P_{dj} = \frac{Context_d}{Context_j} = \frac{A_{d,1} \| \cdots \| A_{d,m}}{A_{j,1} \| \cdots \| A_{j,m}}. \quad (4)$$

Here, $Context_d$ and $Context_j$ represent the context sets of N_d and N_j. To be more precise, we consider a network composed of a set of n nodes $\{n_i\}_{1 \le i \le n}$. Each node's context is defined as a set of attributes $\{A_{i,j}\}_{1 \le j \le m}$.

Energy: Every node possesses limited battery power. It is a critical issue to use battery power efficiently. A node with more battery power can provide more services. Thus, the energy is also serving as a metric to calculate the trust value. We adopt the same method in [21] to detect a neighbor's energy.

4.2. Trust calculation

In this phase, we will introduce how to evaluate or compute the trust value of a target node. In addition to direct and indirect trust, we will discuss the comprehensive trust to balance the weight of direct and indirect decision factors. In Equation (5), we present the trust evaluation from n_i to n_j, $T_{i \to j}$, where α and β represent the weights of social trust metrics S versus QoS trust metrics Q.

$$T_{i \to j} = (S_{i \to j})^{\alpha} \times (Q_{i \to j})^{\beta}. \quad (5)$$

In order to determine the trust level range, a random consistency index, $V = \{v_1, v_2, v_3, v_4\}$, is defined in Table 2. The four elements in V represent 'full trust', 'relative trust', 'general trust' and 'no trust', respectively. These are mapped into [0, 1] with equal intervals.

TABLE 2. Trust level range.

Trust category	Full	Relative	General	No
Psi_{ij}	1–0.75	0.75–0.5	0.5–0.25	0.25–0
Fed_{ij}	1–0.75	0.75–0.5	0.5–0.25	0.25–0

A. *Direct trust*

Based on the direct trust information from target entity, n_i can store n_j's information in the following vector, where destination is the evaluated node.

$$\langle \text{destination}, Psi_{ij}, Fed_{ij} \rangle.$$

Based on the trust degree of each metric, n_i can generate a matrix DT for every destination, where DT_{ij} represents the membership degree from metric i to comprehensive evaluation level j.

$$DT = \begin{pmatrix} DT_{11} & DT_{12} & DT_{13} & DT_{14} \\ DT_{21} & DT_{22} & DT_{23} & DT_{24} \end{pmatrix}. \quad (6)$$

B. *Indirect trust*

Indirect trust means that the evaluating entity indirectly obtains trust information for target entity based on the recommendation from a direct neighbor. However, even after two nodes have built the indirect trust relationship, a node with higher trust value cannot be simply treated as more reliable. This is due to the possibility of collusion attacks, in which the selfish nodes rank the trust values of other selfish nodes higher. To solve this problem, the similarity between two nodes must be used to evaluate the credibility of recommendation. The higher similarity between n_i and n_j is, the higher the credibility of recommendation is.

$RTA_{i \to j}$ is denoted as the trust similarity between n_i and n_j. In Equation (7), A and B represent the trust value sets from their common neighbors, where $A(x_k)$ and $B(x_k)$ are the set elements and z represents the number of their common neighbors.

$$RTA_{i \to j} = \begin{cases} 1 - \frac{1}{z} \sum_{k=1}^{z} |A(x_k) - B(x_k)|, & z > 0, \\ 0.5, & z = 0. \end{cases} \quad (7)$$

ST_{ij} is denoted as the indirect trust relationship. Considering that those nodes with lower recommended credibility may bring a negative impact on the final decision, we calculate the indirect relationship in Equation (8). Here FT_{kj} represents n_k's first hand trust value on n_j. The indirect trust value is

calculated by $RTA_{i\to k}$ and FT_{kj}. RTA_* is used to avoid those recommendations from selfish nodes.

$$ST_{ij} = \begin{cases} RTA_{i\to k} \times FT_{kj}, & RTA_{i\to k} \geq RTA_*, \\ 0, & RTA_{i\to k} < RTA_*. \end{cases} \quad (8)$$

Then, n_i may preserve the indirect trust information ST_{ij} into a matrix IT as follows:

$$IT = \begin{pmatrix} IT_{11} & IT_{12} & IT_{13} & IT_{14} \\ IT_{21} & IT_{22} & IT_{23} & IT_{24} \end{pmatrix}. \quad (9)$$

Here, IT_{ij} represents the membership degree from metric i to comprehensive evaluation level j, either 'full trust', 'relative trust', 'general trust' or 'no trust'.

C. *Comprehensive trust*

In order to alleviate the influence from the subjective evaluation and obtain a more accurate trust value, our model combines direct and indirect trust values. First, the fuzzy evaluation matrix T is given as follows:

$$T = \omega_{dt} \cdot DT + IT. \quad (10)$$

Here, ω_{dt} represents the weight of the direct trust. Since the direct information is relatively important, we can increase the proportion of subjective judgment by increasing ω_{dt}.

Then, we compute the comprehensive trust matrix S and obtain a set of membership values for different nodes as follows:

$$\begin{aligned} S &= W \times T = (s_k)_{1*n} \\ &= (w_{psi}, w_{fed}) \times \begin{pmatrix} T_{11} & T_{12} & T_{13} & T_{14} \\ T_{21} & T_{22} & T_{23} & T_{24} \end{pmatrix}. \end{aligned} \quad (11)$$

In Equation (11), the weight matrix W represents the weight ratio of different metrics with $w_{psi} + w_{fed} = 1$. W should be adjusted as w_{psi} and w_{fed} play different roles. In our scheme, we consider the equal weight, $w_{psi} = w_{fed} = 0.5$. T is a fuzzy matrix and t_{ij} is the membership degree from metric i to comprehensive evaluation level j.

Finally, the trust value from n_i to n_j is evaluated in Equation (12), where $u(v_i)$ represents the indices of the four trust levels in Table 2. For example, if the final trust value is 3.1, the trust value belongs to v_2, 'relatively trust'.

$$Vso_{ij} = \frac{\sum_{i=1}^{n} u(v_i) \cdot {s_i}^k}{\sum_{i=1}^{n} {s_i}^k}, \quad U = \{4, 3, 2, 1\}. \quad (12)$$

4.3. Trust ranking

Every node must rank its neighbors based on weighted average theory before it forwards or shares digital content further. There are two steps for trust ranking.

Step 1: First, every node must get the QoS trust information including C_{ij} (connectivity between n_i and n_j) and E_{ij} (the battery power). Then, every node calculates the QoS trust according to the weight assigned to these metrics.

$$Fqos_{ij} = w_{connectivity} \times C_{ij} + w_{energy} \times E_j. \quad (13)$$

The trust value from n_i to n_j is represented in the following equation:

$$Vfin_{ij} = w_{qos} \times Fqos_{ij} + w_{social} \times Vso_{ij}. \quad (14)$$

Here w_{qos} and w_{social} represent the weight parameter of QoS trust and social trust, respectively, with $w_{qos} + w_{social} = 1$. Social trust is used to decide whether the node is malicious or not, while QoS trust represents the capability of a node to forward messages. The weight parameters aim to balance the two trust metrics. And they can be adjusted in terms of different applications. In Section 5, we will analyze them.

Step 2: The sender ranks other nodes based on the trust value in Equation (14). Only some of the more trusted neighbors will be chosen to forward or share the digital content. The percentage varies with different applications.

4.4. Recovery and mobile firewall mechanism

On one hand, the mobile firewall mechanism is adopted to prevent the spread of viral content. On the other hand, it also serves as an incentive to lure selfish nodes to return to normal behavior again and share multimedia information with others.

After calculation stage, if n_i computes the trust value of n_j to be non-trustworthy, it will broadcast the trust value to all of its neighbors, which will quickly rebroadcast the same message. If a node is detected to be selfish or malicious, it will receive no more messages from other nodes, wasting its stand-by energy. A timer can be set by n_i to reset its trust value of n_j. After the timer expires, n_i can reset its evaluation of n_j to 0.5, giving it a second chance. The timer for the next reset, if necessary, can be doubled.

5. PERFORMANCE EVALUATION

5.1. Simulation configuration

In this section, we use the opportunistic network environment (ONE) simulator [6] to evaluate our trust routing. ONE serves as a powerful tool for generating mobility traces and running simulations with different routing protocols.

In our simulations, we adopt the shortest path map-based movement (SPMBM) model. Dijkstra's shortest path algorithm is to find its way through the map area of Helsinki in Fig. 6. Once a node reaches its destination, it will wait for a predefined pause time. Then a new random map node is chosen and it moves toward the map node based on the shortest path. Furthermore, some points of interest (POIs) are set for the

FIGURE 6. Helsinki simulation area (map data provided by Maanmittauslaitos, 2007).

FIGURE 7. Simulation scenario.

SPMBM model. With those POIs, two nodes will have a better chance to meet if they share some common interests. We assume that every node will be given some context information based on their interests. Then, combining with social and QoS trust, every node will select some neighbors to forward its packets. The simulation scenario is shown in Fig. 7.

To analyze the scheme performance, we focus on the delivery ratio to the destination and the number of transmitted messages. The parameters used in the simulations are summarized in Table 3.

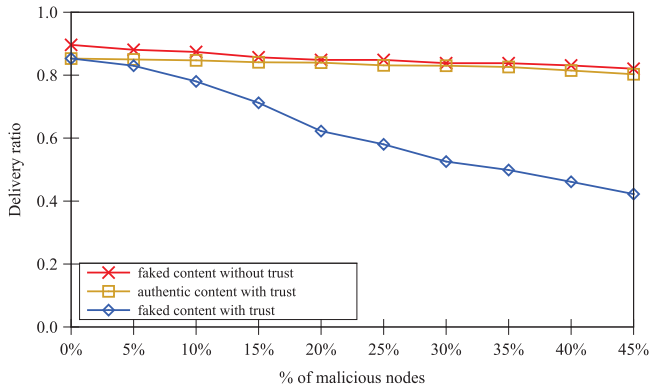

FIGURE 8. Delivery ratios (the lines 'faked content without trust' and 'faked content with trust' represent the delivery ratio of faked content when we use context-based routing without trust model and our trust routing, respectively).

TABLE 3. Parameters used for simulation.

Network area	$4500 \times 3400\,\text{m}^2$
Simulation time	12 h
TTL time	5 hops
Warmup time	1000 s
Number of total nodes	300
Ratio of selfish nodes	0–45%
Speed	1–30 m/s
Transmission rate	2 Mbps
Mobility pattern	SPMBM

5.2. Protection against attack

In this section, we will evaluate our scheme against faked data attack and selfish attack.

A. *Against the faked data attack*

In our simulations, malicious nodes send faked content to a randomly normal node. To investigate the degree of protection against the faked data attack, we compare the delivery ratio of faked and authentic packets. In Fig. 8, the lines 'faked content without trust' and 'faked content with trust' represent the delivery ratio of faked content in a context-based routing [5] and in our model, respectively. And the line 'authentic content with trust' represents the delivery ratio of authentic content.

Figure 8 shows that the delivery ratio of faked content decreases sharply in our trust model. In our model, the creditable feedback of digital content Fed_{ij} is one social trust metric. Once a normal node receives the faked content, it will give a low feedback toward the evaluated node without forwarding and refusing to receive any content from the same evaluated node. Furthermore, other nodes can also distinguish the malicious nodes by using the trust recommendation and

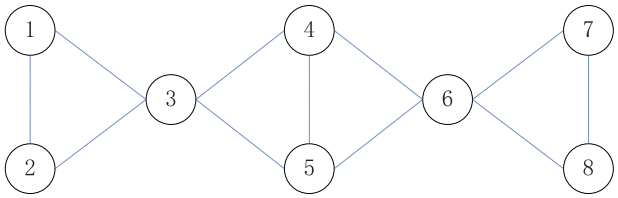

FIGURE 9. Network topology with eight nodes.

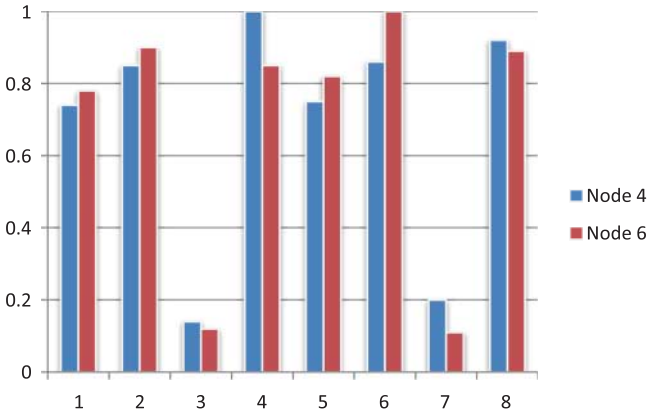

FIGURE 10. Trust values of eight nodes perceived by node 4 and node 6.

mobile firewall mechanisms. In contrast, the delivery ratio of authentic content remains relatively flat. The slight drop is caused by the non-cooperation of the increasing number of malicious nodes. Similarly, the delivery ratio of faked content is flat, implying the necessity to implement a trust model.

B. *Against the selfish node attack*

We combine social trust and QoS trust metrics to evaluate every node's trust degree. We are able to mitigate selfish behaviors by the probability of successful interaction and malicious behaviors by the feedback of digital content. As an illustration, we present a simple wireless network of eight nodes, among which n_3 and n_7 are selfish in Fig. 9.

The trust values perceived by n_4 and n_6 are shown in Fig. 10. We can see that the trust values of n_3 and n_7 are much lower. The normal nodes and selfish nodes can be distinguished obviously.

5.3. Selection of message forwarding rate, λ

In our trust model, only the more trusted neighbors are chosen to forward digital contents. We define λ as a selection rate. A larger λ leads to more message transmission, but higher chance of reaching content destination quickly.

The experimental results are shown in Fig. 11. As λ increases, the message overhead decreases first and then increases. When λ is a small value, the messages are only forwarded to a few nodes, resulting in a lower probability to

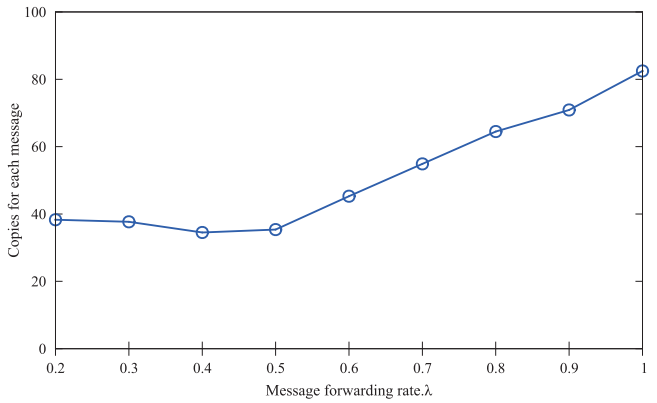

FIGURE 11. Overhead for different message forwarding rate, λ (the number of nodes is $N = 300$. It is obvious that $\lambda = 1$ incurs large overhead for each sending message. The concave shape suggests the existence of an optimum λ).

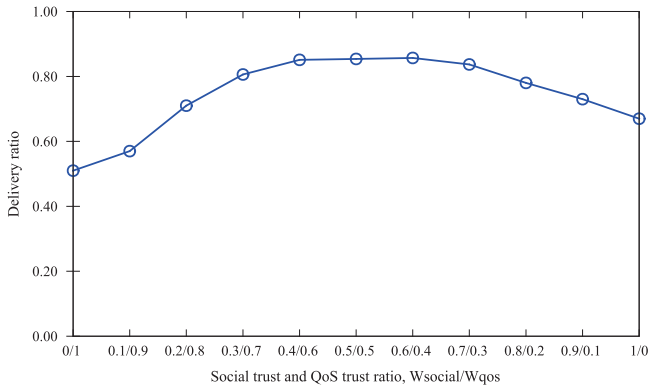

FIGURE 12. Social trust and QoS trust ratio, w_{social}/w_{qos} (the number of nodes is $N = 300$ with 30 selfish nodes).

reach the destination. As λ increases, more nodes are recruited to forward packets. The number of message copies with $\lambda = 1$ is twice as much as the minimum value with $\lambda = 0.4$. During the rest simulations, we will use $\lambda = 0.4$.

5.4. Social trust and QoS trust ratio, w_{social}/w_{qos}

In this section, we evaluate the ratio between social trust and QoS trust, w_{social}/w_{qos}. Here, we consider a network with 250 normal nodes and 30 selfish nodes. The results are shown in Fig. 12.

Social trust contains the probability of successful interactions and the credible feedback of digital content. When the weight of social trust increases, we can select more credible nodes. QoS trust is used to evaluate the capability of a node to deliver messages. The simulation results show that more packets are likely to reach the destination if w_{qos} is increased. According to the results in Fig. 12, the delivery ratio arrives at

the maximum with $w_{social}/w_{qos} = \frac{6}{4}$. Thus, we will choose the ratio $\frac{6}{4}$ for the rest of simulations.

5.5. Impact of selfish nodes

In this section, we analyze the impact of selfish nodes from two aspects: the average hop count and the number of packets dropped. The lower average hop represents that we can send messages successfully with fewer hops. The number of packets dropped shows the impact of selfish nodes.

5.5.1. *Impact on average hop count*

Figure 13 shows the average hop count increases linearly with the selfish nodes. Compared with the protocol [5], Fig. 13 shows that our scheme can achieve the same performance with lower packet overhead.

In Fig. 14, we compare the overhead performance. Overhead is defined as the number of propagated copies for each message. From Fig. 14, we can observe that the overhead of our scheme is less than half of the context-based scheme, which operates without trust. In our trust model, we combine social trust and QoS trust metrics to select next nodes instead of forwarding messages based only on profile information. Furthermore, our scheme can avoid sending messages to selfish nodes by distinguishing selfish and normal nodes. With a fixed λ, our scheme experiences similar overhead even as the selfish node ratio increases.

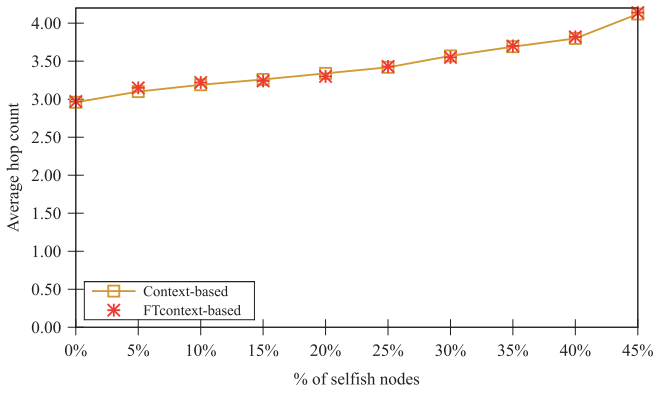

FIGURE 13. Average hop count.

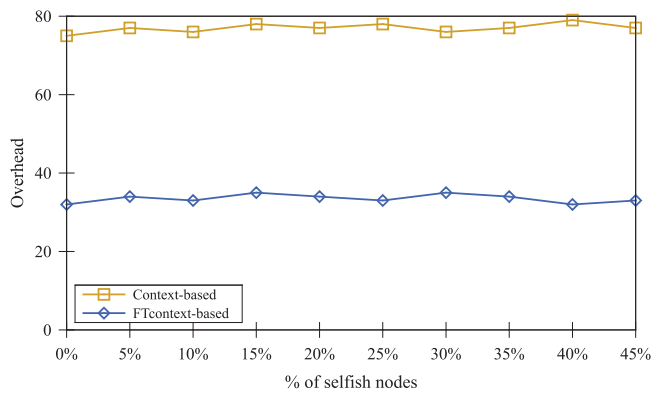

FIGURE 14. Overhead.

5.5.2. *Impact on packet drop rate*

Figure 15 shows the impact of selfish nodes in terms of packet drop rate, which is defined as the number of packets dropped during one message delivery. The packet drop rate in [5] increases with the selfish nodes. When selfish nodes reach 45%, the packet drop rate approximately reaches 100%. Comparatively, the increasing selfish nodes does not have any effect on the packet drop rate in our scheme.

5.6. Protocol comparison

Lastly, we compare our scheme with three state-of-the-art schemes. These are trust-based framework (T-PROPHET) in [2], non-trust-based epidemic (Epidemic) [3] and context-based routing (Context-based) [5]. In T-PROPHET, the positive feedback serves as the evidence of the forwarding behavior of a node. In the epidemic routing scheme, message carriers forward messages to every new encounter. In the context-based routing scheme, message carriers forward messages to the new encounter only when the latter shares some context information with the destination. We compare these protocols from message delivery ratio and balance between delivery ratio and overhead.

Comparisons on message delivery ratio are in Fig. 16. We can see that our protocol and T-PROPHET have less performance degradation than epidemic routing and context-based routing. The reason is that trust models can prevent selfish nodes from receiving messages. Furthermore, the delivery ratio performance in our model is better than T-PROPHET because multimetrics are used.

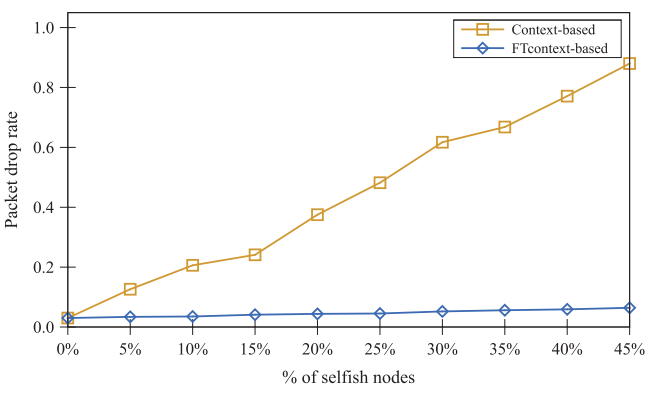

FIGURE 15. Packet drop rate.

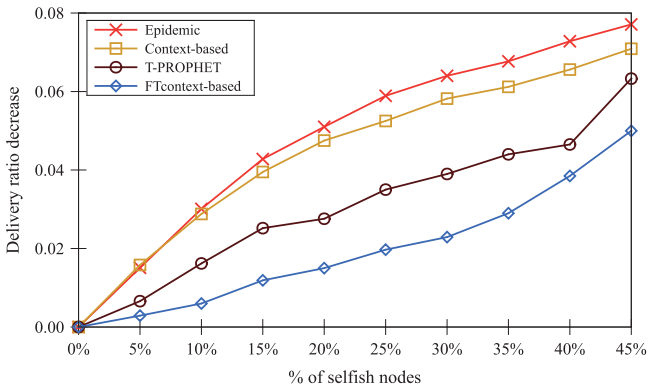

FIGURE 16. Delivery ratio.

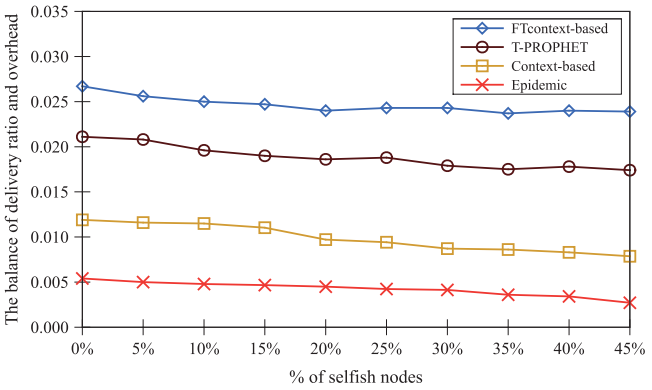

FIGURE 17. The balance of delivery ratio and overhead.

As to the balance between delivery ratio and overhead, we define it as follows:

$$\eta = \frac{\text{Delivery ratio}}{\text{Overhead}}. \tag{15}$$

Larger η means that the delivery ratio can get a higher value with the same overheard cost. As shown in Fig. 17, the results demonstrate that our trust routing can effectively balance the message overhead and delivery ratio.

6. RELATED WORK

In this section, we classify routing protocols into four categories: epidemic routing [3], context-based routing [5], traditional routing [22, 23] and opportunistic routing [24–28].

Epidemic routing [3] relies on flooding the network by sending messages during each encounter. It can guarantee that all messages will be delivered to the destination, if a path exists between source and destination. However, it is wasteful for sending large numbers of redundant messages. Many other attempts have been proposed. For instance, the Probabilistic Routing Protocol [29] uses history of encounters and transitivity to define a probabilistic metric. Then the selection of the best neighbors is based on how frequently they meet each other.

Context-based is proposed to make the routing decision depending on the social connection among nodes. Context information can cover different metrics, depending on different routing protocols [15, 30–33].

In [5], authors focus on the confidentiality and privacy issue. They introduce an original design of a context-based routing protocol. For every node, there are three attributes: mail, workplace and status. End-to-End confidentiality is provided through an extension of identity-based encryption and public encryption with keyword search.

In [31], a BUBBLE protocol is proposed. They exploit two social metrics, namely centrality and community, to make forwarding decisions. In [15], a mobility model based on social network theory is proposed. CAR is proposed in [32] to provide the asynchronous communication in partially connected mobile *ad hoc* networks, based on the intelligent placement of messages. In [33], PROPICMAN is proposed to allow the sender to select forwarders from neighbors such that messages have the highest probability to reach the destination. Three fundamental aspects regarding security, trust and risk are used in [34]. In [1], authors adopt the binary relation rough method based on the rough set and find the rough relation and potential path between communities in MSNs. In [10], a social trust framework for aggregating trust in online social networks is proposed to guarantee the safety management of credible social information by using three key factors. In [11], authors introduce small world characteristics to improve the traditional trust aware recommendation system and to reduce the time complexity. In [12], based on small world theory, shared character factors are used to identify the trust value of every node.

Traditional routing refers to those routing schemes, which find a route for a given packet according to the routing table. It can be further divided into three classes [35]: Destination distance sequence vector [22], *Ad hoc* on-demand distance vector [23] of on-demand driven and hybrid-type routing protocols.

In [7], watchdog and pathrater mechanism are proposed based on promiscuous mode operation of the nodes. In [8], RFSTrust, a trust model based on fuzzy recommendation similarity, is proposed to quantify and to evaluate the trustworthiness of nodes, which includes five types of fuzzy trust recommendation relationships based on the fuzzy relation theory and a mathematical description for MANETs. In [36], a CONFIDANT protocol based on the traditional routing DSR is proposed to evaluate each node in the same way of watchdog.

Opportunistic routing is an upcoming routing technique for wireless networks. The key concept behind opportunistic routing is overhearing and cooperation among relaying nodes [24–28].

In [2], authors design a trust-based framework PROPHET to more accurately evaluate an encounter's delivery competency,

which can be flexibly integrated with a large family of existing data forwarding protocols designed for OppNets. The positive feedback message is proposed as the evidence of the forwarding behavior of a node.

In [25], authors have introduced a framework to analyze the one-hop throughput of geographic opportunistic routing. In [26], ECONOMY is proposed to utilize overheard packets and to take multiple routes into consideration. In [24], a CCACK scheme is proposed. CCACK allows nodes to acknowledge network-coded traffic to their upstream nodes in a simple way, oblivious to loss rates and with negligible overhead.

Because a social network is a structure of nodes that are connected [37] with each other via certain types of relations, such as friendship, workplace and hobbies, context-based forwarding [5] is usually used. Using the context as heuristic is interesting for controlling epidemic forwarding. Every node decides to forward a message only if the shared context between itself and the destination is significant.

7. CONCLUDING REMARKS

The trust relationship between nodes has a direct impact on the sharing and transmission method of digital content. To efficiently route packets, we have investigated trust model and routing scheme in the MSN environment to guarantee the routing validity and avoid some selfish or malicious nodes. We adopt fuzzy sets to establish a new trust evaluation model based on the multimetrics. Combining direct trust and indirect trust relationship, every node can rank all its neighbors. During the routing decision, the untrustworthy nodes will be ignored. We have analyzed and evaluated our trust routing with the ONE simulator. Security analysis shows that our protocol can meet the security requirements. Simulation results show that our routing protocol possesses several unique properties on delivery probability and traffic overhead.

In future work, we will conduct further studies on the anti-attack capacity and incorporate other influencing attributes into the trust model.

FUNDING

This research is sponsored in part by the National Natural Science Foundation of China (contract/grant number: No. 61173179 and No. 61202441) and Program for New Century Excellent Talents in University (NCET-13-0083). This research is also sponsored in part by the Fundamental Research Funds for the Central Universities (No. DUT13JS10 and No. DUT14YQ212).

REFERENCES

[1] Yang, L., Zhang, Z. and Pu, L. (2012) Rough set and trust assessment-based potential paths analysis and mining for multimedia social networks. *Int. J. Digit. Content Technol. Appl.*, **6**, 640–647.

[2] Na, L. and Das, S.K. (2013) A trust-based framework for data forwarding in opportunistic networks. *Ad Hoc Netw.*, **11**, 1497–1509.

[3] Vahdat, A. and Becker, D. (2000) Epidemic Routing for Partially Connected Ad Hoc Networks. Technical Report CS-2000-06. Duke University, Durham NC, USA.

[4] Nguyen, H.A. and Giordano, S. (2012) Context information prediction for social-based routing in opportunistic networks. *Ad Hoc Netw.*, **10**, 1557–1569.

[5] Shikfa, A., Onen, M. and Molva, R. (2010) Privacy and confidentiality in context-based and epidemic forwarding. *Comput. Commun.*, **33**, 1493–1504.

[6] Azzedin, F. and Ridha, A. (2007) Fuzzy trust for peer-to-peer based systems. *World Acad. Sci.*, **21**, 123–127.

[7] Marti, S., Giuli, T.J., Lai, K. and Baker, M. (2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *Int. Conf. Mobile Computing and Networking*, Boston, MA, USA, August 6–11, pp. 31–38. ACM, USA.

[8] Luo, J., Liu, M. and Fan, M. (2000) A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Comput. Netw.*, **53**, 2396–2407.

[9] Bharadwaj, K.K. and Al-Shamri, M.Y.H. (2009) Fuzzy computational models for trust and reputation systems. *Electron. Comm. Res. Applic.*, **8**, 37–47.

[10] Caverlee, J., Liu, L. and Webb, S. (2010) The SocialTrust framework for trusted social information management: architecture and algorithms. *Inf. Sci.*, **180**, 95–112.

[11] Yuan, M., Guan, D., Lee, Y.K., Lee, S. and Hur, S.J. (2010) Improved trust-aware recommender system using small-worldness of trust networks. *Knowl.-Based Syst.*, **23**, 232–238.

[12] Zhang, Z. and Wang, K. (2013) A trust model for multimedia social networks. *Soc. Netw. Anal. Min.*, **3**, 969–979.

[13] Ouyang, K.X., Vaidya, B. and Makrakis, D. (2002) A Probabilistic-Based Approach Towards Trust Evaluation Using Poisson Hidden Markov Models And Bonus Malus Systems. *2011 9th Annual Int. Conf. Privacy, Security and Trust (PST)*, Quebec, Canada, July 19–21, pp. 150–155. IEEE, USA.

[14] Ghosh, A. and Bhattacharya, S. (2013) Calculating trust and aggregation of a node using Poisson distribution in WSN. *Int. J. Comput. Appl.*, **68**, 43–47.

[15] Musolesi, M. and Mascolo, C. (2006) A Community Based Mobility Model for Ad Hoc Network Research. *REALMAN '06 Proc. 2nd Int. Workshop on Multi-Hop Ad Hoc Networks: From Theory to Reality*, Florence, Italy, May 26–26, pp. 31–38. ACM, USA.

[16] Bede, B. (2013) *Mathematics of Fuzzy Sets and Fuzzy Logic*. Springer, Berlin.

[17] Luo, J., Liu, X. and Fan, M. (2009) A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Comput. Netw.*, **53**, 2396–2407.

[18] Su, X., Zhang, M., Mu, Y. and Bai, Q. (2012) A robust trust model for service oriented systems. *J. Comput. Syst. Sci.*, **79**, 596–608.

[19] Chen, D., Chang, G., Sun, D., Li, J. and Jia, J. (2011) TRM-IoT: a trust management model based on fuzzy reputation for internet of things. *Comput. Sci. Inf. Syst.*, **8**, 1207–1228.

[20] Jøsang, A., Lsmail, R. and Boyd, C. (2007) A survey of trust and reputation systems for online service provision. *Decis. Support Syst.*, **43**, 618–644.

[21] Vidhyapriya, R. and Vanathi, P.T. (2007) Energy Aware Routing for Wireless Sensor Networks. *Int. Conf. Signal Processing, Communications and Networking. ICSCN'07. IEEE*, Chennai, India, February 22–24, pp. 545–550. IEEE, USA.

[22] Wan, T., Kranakis, E. and Van Oorschot, P.C. (2004) Securing the Destination Sequenced Distance Vector Routing Protocol (S-DSDV). Lect. Notes in Comput. Sci., **3269**, 358–374.

[23] Perkins, C.E. and Royer, E.M. (1999) Ad-Hoc on-Demand Distance Vector Routing. *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, Louisiana, USA, February 25–26, pp. 90–100. IEEE, USA.

[24] Koutsonikolas, D., Wang, C.C. and Hu, Y.C. (2011) Efficient network-coding-based opportunistic routing through cumulative coded acknowledgments. *IEEE/ACM Trans. Netw.*, **19**, 1368–1381.

[25] Zeng, K., Lou, W., Yang, L. and Brown, D.R. (2007) On throughput efficiency of geographic opportunistic routing in multihop wireless networks. *Mob. Netw. Appl.*, **12**, 347–357.

[26] Hsu, C.J., Liu, H.I. and Seah, W. (2009) Economy: A Duplicate Free Opportunistic Routing. *Proc. 6th Int. Conf. Mobile Technology, Application and Systems*, Nice, France, September 10–13, pp. 1–6. ACM, USA.

[27] Lin, Y., Liang, B. and Li, B. (2010) SlideOR: Online Opportunistic Network Coding in Wireless Mesh Networks. *IEEE Conf. Computer Communications (INFOCOM)*, San Diego, USA, March 14–19, pp. 1–5. IEEE, USA.

[28] Hsu, C. J., Liu, H. I. and Seah, W. K. (2011) Opportunistic routing—a review and the challenges ahead. *Comput. Netw.*, **55**, 3592–3603.

[29] Lindgren, A., Doria, A. and Schelen, O. (2003) Probabilistic routing in intermittently connected networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, **7**, 19–20.

[30] Nguyen, H.A. and Giordano, S. (2011) Routing in opportunistic networks. *Ubiquit. Dev. Ambient Comput. Intell.: Hum.-Centered Appl.*, **13**, 179–193.

[31] Hui, P., Crowcroft, J. and Yoneki, E. (2011) Bubble rap: social-based forwarding in delay-tolerant networks. *Mob. Comput.*, **10**, 1576–1589.

[32] Musolesi, M., Hailes, S. and Mascolo, C. (2005) Adaptive Routing for Intermittently Connected Mobile Ad Hoc Networks. *Sixth IEEE Int. Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Taormina, Italy, June 16–16, pp. 183–189. IEEE, USA.

[33] Nguyen, H.A., Giordano, S. and Puiatti, A. (2007) Probabilistic Routing Protocol for Intermittently Connected Mobile Ad Hoc Networks (PROPICMAN). *IEEE Int. Symp. World of Wireless, Mobile and Multimedia Networks*, Helsinki, Finland, June 18–21, pp. 1–6. IEEE, USA.

[34] Zhang, Z. (2012) *Security, Trust and Risk in Digital Rights Management Ecosystem*. Science Press, Beijing.

[35] Bakht, H. (2011) Survey of routing protocols for mobile ad hoc networks. *Int. J. Inf. Commun. Technol. Res.*, **1**, 258–270.

[36] Buchegger, S. and Le Boudec, J.Y. (2002) Performance Analysis of the Confidant Protocol. *Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, Lausanne, Switzerland, June 9–11, pp. 226-236. ACM, USA.

[37] Zhao, H.V., Lin, W.S. and Liu, K.R. (2009) Behavior modeling and forensics for multimedia social networks. *Signal Process. Mag.*, **26**, 118–139.