Wireless Networks (2019) 25:3587–3603
https://doi.org/10.1007/s11276-019-01955-2

Novel approach of distributed & adaptive trust metrics for MANET

De-gan Zhang[1,2,3] · Jin-xin Gao[1,2] · Xiao-huan Liu[1,2] · Ting Zhang[1,2] · De-xin Zhao[1,2]

Published online: 20 March 2019

Abstract

It is known to all that mobile ad hoc network (MANET) is more vulnerable to all sorts of malicious attacks which affects the reliability of data transmission because the network has the characteristics of wireless, multi-hop, etc. We put forward novel approach of distributed & adaptive trust metrics for MANET in this paper. Firstly, the method calculates the communication trust by using the number of data packets between nodes, and predicts the trust based on the trend of this value, and calculates the comprehensive trust by considering the history trust with the predict value; then calculates the energy trust based on the residual energy of nodes and the direct trust based on the communication trust and energy trust. Secondly, the method calculates the recommendation trust based on the recommendation reliability and the recommendation familiarity; adopts the adaptive weighting, and calculates the integrate direct trust by considering the direct trust with recommendation trust. Thirdly, according to the integrate direct trust, considering the factor of trust propagation distance, the indirect trust between nodes is calculated. The feature of the proposed method is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Simulation experiments and tests of the practical applications of MANET show that the proposed approach can effectively avoid the attacks of malicious nodes, besides, the calculated direct trust and indirect trust about normal nodes are more conformable to the actual situation.

Keywords Mobile Ad hoc Network · Distributed · Adaptive · Trust metrics · Malicious attacks

1 Introduction

Mobile ad hoc network (MANET) is a kind of wireless mobile communication network composed of logical equivalence mobile nodes with wireless transceiver [1]. It does not rely on any default infrastructure, but through the collaboration among the mobile nodes with limited communication scope to maintain the network connectivity and realize the data transform [2, 3]. Its characteristics are as follows: mobility, multi-hop, self-organizing, distributed control, wireless, dynamic topology, limited link bandwidth and the limited calculation ability [4–7]. When the distance of the two nodes is larger than the range of one hop communication radius, the two nodes can conduct multi-hop communication by using others as intermediate nodes. Figure 1 shows a simple structure of self-organizing network topology. Because of the limitation of communication radius, node 1 and node 5 cannot communicate directly, but they can conduct multi-hop communication by using others as intermediate nodes on the path.

✉ Xiao-huan Liu
815215568@qq.com

De-gan Zhang
gandegande@126.com; zhangdegan@tsinghua.org.cn

Jin-xin Gao
974281483@qq.com

Ting Zhang
gandegande@126.com

De-xin Zhao
1327363190@qq.com

[1] Key Laboratory of Computer Vision and System, Ministry of Education, Tianjin University of Technology, Tianjin 300384, China

[2] Tianjin Key Lab of Intelligent Computing & Novel Software Technology, Tianjin University of Technology, Tianjin 300384, China

[3] School of Electronic and Information Engineering, University of Sydney, Sydney, NSW 2006, Australia

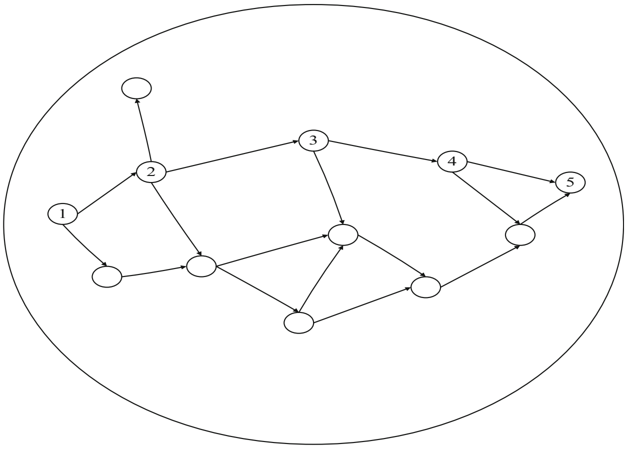


Fig. 1 One simple structure of MANET

Since MANET has the characteristics of flexible using, rapid networking and strong robustness, etc. It can be widely used in the field of civilian emergency rescue, medical health monitoring and military battlefield rescue [8–10], etc. However, the characteristics of MANET makes the network more vulnerable to malicious attacks. So it is very important to ensure the data security of MANET.

Nowadays, a variety of security mechanisms have been proposed to deal with hacking attack, data forgery attack, such as security authentication, verification of the integrity of message, message encryption mechanism, etc. [11–15]. But these methods are not effectively against many other attacks, such as node capture attack, denial of service attack, etc. Traditional security mechanisms can effectively resist the external attacks, but for internal attacks caused by node captured, the efficiency of the resistance is lower. In order to guarantee communication security, we need to select a node which within the communication scope of forwarding nodes to transmit data. In this way, we can make sure the data transmission more security.

Our method calculates the communication trust by using the number of data packets between nodes, predicts the trust based on the trend of this value, and calculates the comprehensive trust by considering the history trust with the predicted value; then calculates the energy trust based on the residual energy of nodes and the direct trust based on the communication trust and energy trust. The detection process of our method can help to mitigate the various attack types mentioned in the paper. The technology is called activity- based overhearing, iterative probing, and unambiguous probing. Our proposed trust calculation attempts to resolve the relative issue by adopting a dynamic source routing mechanism. The experiments show that our proposed approach can effectively avoid the attacks of malicious nodes, besides, the calculated direct trust and indirect trust about normal nodes are more conformable to the actual situation.

2 Related work

At present, many kinds of trust models have been put forward to calculate the trust value between nodes, to achieve the purpose of reliable data transmission [16–21]. Literature [22] proposed a Parameter and Localized trUst management Scheme named PLUS. It considered the direct trust and recommendation trust comprehensively when the distance of two nodes is smaller than the communication radius. Within the scope of each region, PLUS sets a judge node to evaluate the trust value of every node. Source node sends the data to the judge, and the judge node would test the integrity of packets. If the packet integrity fails in the test, the judge node decreases the trust value of this source node without considering whether it is really a malicious node. Therefore, the calculated trust value may not be accurate enough. Literature [23] proposed a node behaviors between trust evidence (NBBTE) algorithm based on the D-S trust theory. In NBBTE, first of all, according to the history communication behaviors between neighbor nodes, it sets up various communications trust factors. Then, it calculates the direct trust between nodes by using the fuzzy set theory. Finally, considering the recommendation trust between nodes, NBBTE calculates the integrate trust by using the theory of D-S, direct trust and recommendation trust. Literature [24] proposed an extended distributed trust model (EDTM) for wireless sensor networks. This model is divided into two modules: when the distance is smaller than the communication radius, it enters into one-hop module; otherwise, it enters into multiple-hop module. One-hop module contains the calculation of direct trust and recommendation trust, and multiple-hop module contains the calculation of indirect trust [25–27]. To the best of our knowledge, NBBTE and EDTM are relatively better, NBBTE and EDTM performs better than other algorithms [28–32]. So we will compare our algorithm (namely DATEA) with these two methods in the experiments.

According to the above analysis, we can find that [33–37]: 1) It is not completely reliable to calculate the trust value just considering the communication behavior between nodes. We also need to consider the energy. Only if the nodes have enough energy, they have enough ability to transmit the data. 2) When the distance of two nodes is smaller than that of the communication radius, the calculation of trust contains not only direct trust but also recommendation trust. The recommendation trust is achieved from the common neighbors of these two nodes. But not all of the recommendations are reliable; there might be malicious or exaggerated recommendation. So we need to analyze the recommendation trust of the node. A more reliable calculation of the recommendation trust depends on the recommendation reliability and recommendation familiarity. 3) Due to the characteristics of mobility and dynamic topology of MANET, the existing methods to calculate the trust are not good enough to solve the problem of the real-time and the trend of trust value. 4) In view of multiple-hop, self-organizing, trust propagation distance is not considered in those proposed methods to evaluate indirect trust. In order to solve some aforementioned problems, we propose an approach of distributed and adaptive trust evaluation (DATEA) for MANET in this paper.

3 Network model

3.1 Topology of the network

Assuming the applicable network has the following characteristics [38–42]: The area of the network topology is $M \times M$, where M is a limited positive integer that is used to local an area for modeling, and the number of nodes in this area is *NodeNums*. All the nodes are randomly distributed in the area. Every node generates data and randomly transmits data to others. As shown in Fig. 2, in this multiple-hop network, nodes are divided into three categories: the source node, the destination node and the forwarding node. The source node can directly communicate with the other nodes within the communication radius of the source node. Otherwise, it needs the forwarding nodes to transmit data.

At the same time, we assume that the nodes have the following features [43–47]: Each node has a unique ID; Each node has the same initial energy, capability of communication and computing, and the same storage capacity; The nodes have the ability of location-aware, with Beidou device or GPS device or other devices (nowadays, these devices are very common, the calculation of trust is distributed, if the GPS coordinates of all nodes may be expensive to achieve, the cheaper Beidou coordinates can be used to replace GPS coordinates); The nodes calculate the distance between nodes according to their location; Each node stores ID of its neighbor nodes within communication radius; The nodes can adjust the transmission power according to the communication distance; With the multi-hop feature, every node only can directly communicate with their neighbor nodes within communication radius [48–51].

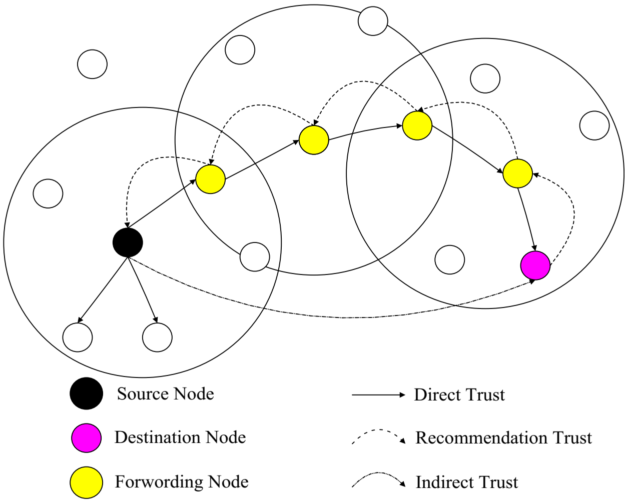


Fig. 2 Node category structure in Multi-hop network

3.2 Model of the energy consumption

A typical node is mainly composed of four modules: data sensing unit, communication unit, processing unit and batteries. The energy consumption is shown in Fig. 3.

As shown in Fig. 3, the communication unit has the largest proportion of total energy consumption, and the transmit unit consumes the most energy, receive unit and monitor are less than transmit unit, and the sleep state has the minimum energy consumption. The energy consumption of sensing and processing units are far less than the communication unit. So, compared with the total energy consumption, the energy consumption of sensing and processing unit can be neglect. According to the radio consumption model [25–27], after transmits a k-bit message, the formula of energy consumption is as follows.

$$E_{Tx}(k,d) = E_{Tx-elec}(k) + E_{Tx-amp}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{f}s \times d^2 & d \le d0 \\ kE_{elec} + k\varepsilon_{mp} \times d^4 & d > d0 \end{cases} \tag{1}$$

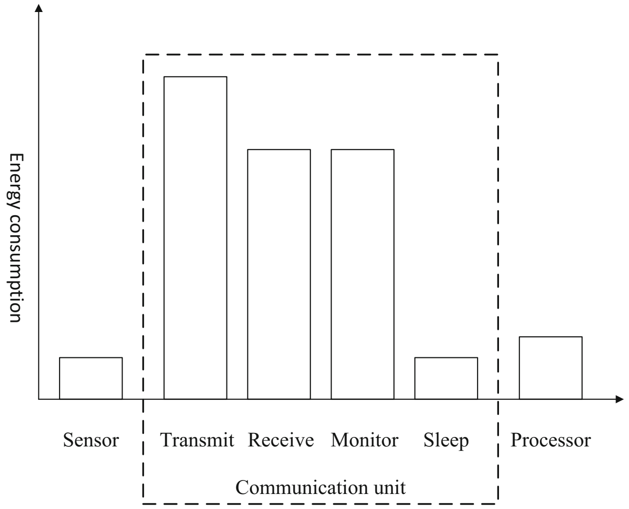


Fig. 3 Energy consumption distribution of WSN

where $d0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$, k is the number of transferred bytes, d is the transmission distance. When the transmission distance is smaller than d_0, the power amplification adopts free-space mode, otherwise adopts the multi-fading model. E_{elec}(nJ/bit) is the energy coefficients of radio frequency. ε_{fs} and ε_{mp} are coefficient of energy consumption of two modes of amplifier circuit.

Receiving a k-bit message, the formula of energy consumption is as follows.

$$E_{Rx}(k) = E_{Rx-elec}(k) = kE_{elec} \tag{2}$$

As we know, the above Eqs. (1) and (2) are realistic power consumption model of wireless subsystems typically used in many sensor communication node devices. Simple power consumption models for major components are individually identified, and the effective transmission range of a sensor node is modeled by the output power of the transmitting power amplifier, sensitivity of the receiving low noise amplifier. Using this basic model, conditions for minimum sensor network power consumption are derived for communication of sensor data from a source device to a destination node. Power consumption model parameters are extracted for two types of wireless sensor nodes that are widely used and commercially available. It is shown that whenever single hop routing is possible it is always more power efficient than multi-hop routing. Single hop routing will be more power efficient compared to multi-hop routing under realistic circumstances. This power consumption model can be used to guide design choices at many different layers of the design space including topology design, node placement, energy efficient routing schemes, power management and the design of wireless sensor network devices.

3.3 Attack model

Malicious attacks on MANET include the following kinds: Denial of service (DoS) attack, data forgery attack, Sybil attack, flooding, selective forwarding attack, bad/good-mouthing attack, wormhole attack, etc. Like bad/good-mouthing attack, if the source node wants to get the integrate trust value of destination, it has to get the recommendation trust from the third party. If the third party is the malicious node, namely the third party maliciously describes the destination node and decreases the recommendation trust about destination node, then the integrate trust between source and destination node will be decreased. On the other hand, if the third party exaggerates the recommendation trust about destination node, the comprehensive trust will be increased. To sum up, there is a difference between recommendation trust and the actual value. This work adopts the flooding, the bad/good-mouthing, and the selective forwarding attack into our experiments.

4 Specific design of DATEA

4.1 Structure of trust model

Definition 1 Trust. Through communication behavior of packets transmission between nodes, we calculate the integrated trust by factors including packet loss rate, energy of nodes and the recommendation trust, and it is called trust of node. The range of trust value is set from 0 to 1, and 0 is distrust completely, 1 is trust completely. Characteristics of Trust: Asymmetry, transitivity and composability. Asymmetry, if node A trusts node B, it does not necessarily means that node B trusts node A. Transitivity implies that if node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a center level. Composability means that trust values received from multiple available paths can be composed together to obtain an integrated value.

4.1.1 One-hop trust module

When the source node wants to obtain the trust value aims at destinations, first of all, it calculates the distance between nodes based on the location. If the distance is smaller than communication radius, enter into one-hop module. One-hop module contains direct trust module and recommendation trust module. Direct trust module contains communication trust module and energy trust module.

Definition 2 Communication Trust. When the distance between source nodes and destination nodes is smaller than that of the communication radius, they can transmit data directly. Based on the number of transferred data packets, the communication trust can be calculated.

Definition 3 Energy Trust. When the source nodes send message to destination nodes, the trust is calculated based on the neighbors' remain energy, to make sure that the forwarding nodes have the ability to receive and forward data packets.

Definition 4 Direct Trust. When the distance between source nodes and destination nodes is smaller than that of the communication radius, by combining communication trust with energy trust, the direst trust between nodes can be calculated.

Definition 5 Recommendation Trust. When the distance between source and destination nodes is smaller than that of the communication radius, they can directly transmit data packets. But if the number of communication packets is not large enough, just calculating the direct trust may not be able to correctly reflect the actual trust value. Set the common neighbors of source and destination nodes as the third party, and the third party provides their own trust aim at destinations to the source nodes, the provided trust is called recommendation trust.

Therefore, in one-hop module, the integrate trust between nodes depends on two aspects: direct trust and recommendation trust. If the number of communication packets is larger than or equal to the threshold, only the direct trust needs to be computed. Otherwise, the direct and recommendation trust need to be comprehensively calculated.

4.1.2 Multi-hop trust module

When the distance between source and destination nodes is larger than that of the communication radius, with the characteristic of multi-hop, establishing a transfer path by using other intermediate nodes, and depending on the direct trust and trust propagation, the indirect trust between source and destination nodes can be obtained.

4.1.3 Trust update module

Since MANET has the characteristics of dynamic topology and self-organizing, the nodes would join and exit network randomly. So the trust between nodes needs to be updated in real time. The trust evaluation model is as shown in Fig. 4.

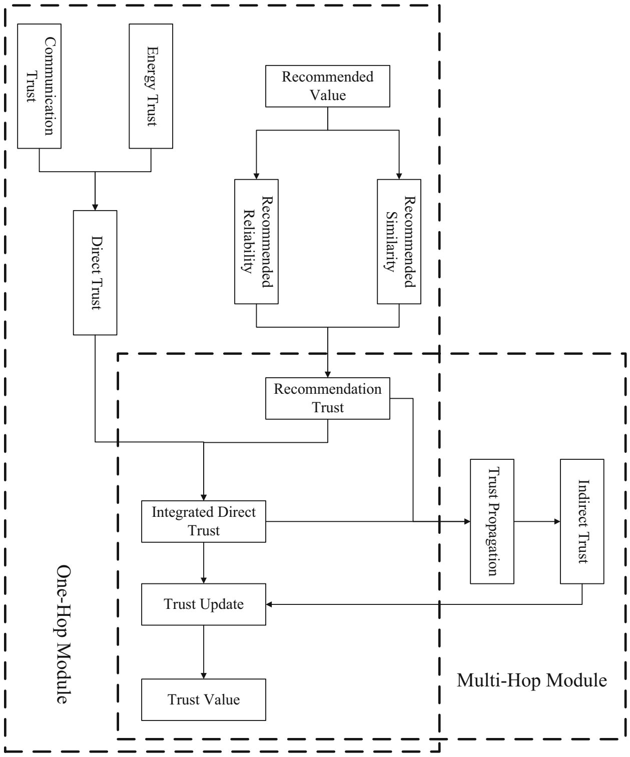


Fig. 4 The structure of DATEA

4.2 Calculation of direct trust

We use the number of communication packets between nodes to calculate the communication trust. But with various internal or external interference, it is not accurate enough to calculate the direct trust just based on communication trust. The node consumes a certain amount of energy after transmits a data packet. Normally, the energy consumption rate is quantitative or fluctuates within a certain tolerance. But if the node is damaged or attacked, the energy consumption rate will be largely difference with normal nodes. Like flooding, the node sends large numbers of packets, the energy consumption will be very large, and the energy consumption rate per unit of time is bigger than the rate of normal nodes. On the other hand, because of the characteristic of selfish, the selfish-node does not forward data packets, so its energy consumption rate is smaller than the rate of normal nodes [26].

4.2.1 Calculation of communication trust

Calculate the communication trust based on the number of successful communication packets. Assume that s is the number of successful communication packets; f is the number of unsuccessful communication packets. According to the subjective logic framework (SLF) theory [27], trust is composed by 3-dimensional vector $T = \{b,d,u\}$. The parameters b,d,u respectively represents trust, distrust and uncertain. $b,d,u \in [0, 1]$, $b + d + u = 1$. The calculation formula is shown as follows.

$$\begin{aligned} T_{fwd1} &= \frac{2b+u}{2} \\ T_{drp1} &= \frac{2d+u}{2} \\ T_{fls1} &= u \end{aligned} \tag{3}$$

where $b = \frac{s}{s+f+1}, d = \frac{f}{s+f+1}, u = \frac{1}{s+f+1}$,$T_{fwd1}$ is forward packet trust, T_{drp1} is drop packet trust, T_{fls1} is uncertain factors trust.

According to the Eq. (3) with SLF theory, the trust networks consist of transitive trust relationships, e.g. as reputation scores or as subjective trust measures, trust between parties within the community can be derived by analyzing the trust paths linking the parties together. Trust network analysis using subjective logic provides a simple notation for expressing transitive trust relationships, and defines a method for simplifying complex trust networks so that they can be expressed in a concise form and be computationally analyzed. Trust measures are expressed as beliefs, and subjective logic is used to compute trust between arbitrary parties in the network.

Because of the dynamic topology, the trust between nodes changes along with the network status in MANET. Just relying on the history number of communication packets to calculate the trust between nodes may not be able to reflect the actual value. Introducing aggregative reputation (AR) model to predict the trust value [28, 29], combining history trust value with predict trust, the comprehensive communication trust can be obtained. The AR is a regression model, based on the past p status before current moment, by using a set of linear prediction formulas to predict the communication trust at the next moment.

$$\begin{aligned}T_{fwd}(t) &= K_1 + W_1 \times \sum_{i=1}^{p} T_{fwd}(t-i) + E_1(t)\\ T_{drp}(t) &= K_2 + W_2 \times \sum_{i=1}^{p} T_{drp}(t-i) + E_2(t)\\ T_{fls}(t) &= K_3 + W_3 \times \sum_{i=1}^{p} T_{fls}(t-i) + E_3(t)\end{aligned} \tag{4}$$

where T_{fwd} is forward packet trust, T_{drp} is drop packet trust, T_{fls} is uncertain factors trust. W_1, W_2, W_3 are weight values, $E_1(t)$, $E_2(t)$, $E_3(t)$ are noise, K_1, K_2, K_3 are constants which usually can be neglect to simplify the calculation. From formula (4) we can calculate the node trust at moment t after obtaining W_i and p. For W_i, there are many difference algorithms, such as least squares, canonical equations, etc. p is the size of sample set. Normally, it is considered that the larger size of sample set, the more accurate the trust value is. Actually, if the sample is too early, the calculated trust cannot reflect the actual trust at that moment. p is calculated by Final Prediction Error Criteria or Akaike Information Criterion (AIC). Here we adopt the least squares to calculate W_i and adopt AIC to calculate p.

According to the above theory, we can obtain the formula as follows.

$$\begin{aligned}T_{fwd} &= k_1 \times T_{fwd1} + k_2 \times T_{fwd}(t)\\ T_{drp} &= k_3 \times T_{drp1} + k_4 \times T_{drp}(t)\\ T_{fls} &= k_5 \times T_{fls1} + k_6 \times T_{fls}(t)\end{aligned} \tag{5}$$

where k_1, k_2, k_3, k_4, k_5 and k_6 are weights. T_{fwd1}, T_{drp1}, T_{fls1} respectively represents forward packet trust, drop packet trust and uncertain factors trust at present. $T_{fwd}(t)$, $T_{drp}(t)$, $T_{fls}(t)$ respectively represents forward packet trust, drop packet trust and uncertain factors trust at time t.

The Eq. (5) with Akaike Information Criterion has had an important impact in statistical model evaluation problems. We studied the general theory of the AIC procedure and provided its analytical extensions in two ways without violating the main principles. Asymptotic properties of AIC and its extensions are investigated, and empirical performances of these criteria are studied in choosing the correct degree of a polynomial model in two different Monte Carlo experiments under different conditions.

Calculating the instant communication trust based on Subjective Logic Framework, predict the communication trust based on AR model. The integrate communication trust computed by combining the instant trust with the predict trust is more real-time and more in line with the dynamic characteristic of topological structure.

For example, at the initial state, node B and C are one-hop neighbors of node A. And the distance between A and B is smaller than the distance between A and C. So, at the initial state, the number of communication packets between A and B is larger than that between A and C. Then the calculated trust between A and B is larger. Due to the dynamic characteristic, the factors like congestion may lead the trust between A and B to trend to decrease (0.9 → 0.8 → 0.7 → 0.6). With many factors, the number of successful communication packets between A and C may increase. So the communication trust between A and C trends to increase (0.3 → 0.4 → 0.5 → 0.6). Only based on SLF, the communication trust obtained between A and B is 0.6, the trust between A and C is 0.6 either. At this moment node A is confused to transmit packets to B or C. By using AR model, the trust value obtained between A and B is 0.5, and the trust between A and C is 0.7. Combine the trust obtained from SLF with the predict value obtained from AR, and respectively set the weight of SLF and AR to 1/2. The integrate communication trust obtained between A and B is 0.55, and 0.65 between A and C. So, node A is going to sends the packets to C.

Combine SLF with AR, set $b = T_{fwd}$, $d = T_{drp}$, $u = T_{fls}$. The formula to calculate the comprehensive communication trust is as follows.

$$T_{com} = \frac{2T_{fwd} + T_{fls}}{2} \tag{6}$$

4.2.2 Calculation of energy trust

Under the condition of invariable environment in the network, the energy consumption rate of node is basically stable after sending or receiving a certain message, or the rate fluctuates with a certain tolerance. However, if the node is malicious, such as flooding, then the energy consumption rate is much bigger than the rate of normal nodes. On the other hand, because of the characteristic of selfish, the selfish-node does not forwards data packets, so its energy consumption rate is smaller than the rate of normal nodes.

According to the energy consumption model, the energy trust can be calculated by obtaining the residual energy of nodes. The calculation formula of the energy trust is as follows.

$$T_{ene} = \begin{cases} \frac{1}{N_{ij}} \times \frac{E_{ij}}{E_{aveij}} & if \quad E_{ij} \geq \theta \\ 0 \quad else & \end{cases}$$
$$E_{avgij} = \frac{1}{N_{ij}} \times \sum_{j=1}^{N_{ij}} E_{ij} \tag{7}$$

where node j is a neighbor node of node i. E_{ij} is the residual energy of node j. N_{ij} is the number of neighbors of node i. E_{aveij} is the average residual energy of all the neighbor node j. θ is the threshold of residual energy. With the characteristics of mobility and dynamic topology, the neighbor nodes continual change.

The threshold need to be adaptively adjusted, so we set $\theta = \frac{E_{aveij}}{2}$.We set the adaptive threshold to make sure neighbor nodes live longer and the entire network is longer. The Eq. (7) is obtained by us based on our analysis & deduction and relative experiments under different conditions.

Based on the calculation formula of energy trust and adaptively adjust the threshold, the calculated energy trust is much more in line with the dynamic topology of network, and helps to extend the survival time of nodes.

For example, Node i has 5 neighbors within the scope of one-hop, and their residual energy are 0.2, 0.4, 0.7, 0.9 and 0.5 respectively. By using the above formula (7) to calculate the energy trust, we obtain the trust are 0, 0.148, 0.26, 0.34 and 0.185 respectively. It can be found that the node with largest energy 0.9 has the largest energy trust. Besides, if there are 4 neighbors with the scope of one-hop and their residual energy respectively are 0.2, 0.2, 0.2 and 0.8, by using the above formula (7) to calculate the energy trust, the trust obtained are 0.143, 0.143, 0.143 and 0.57. It is also found that the node with largest energy 0.8 has the largest energy trust. Therefore, the above formula (7) can effectively calculate the energy trust of each node, and choose the most reliable nodes as the next forwarding nodes. In this way, it can effectively prolong the survival time of nodes.

Integrating the communication trust and the energy trust. When the distance between source node and destination node is smaller than that of the communication radius, the formula to calculate the direct trust is as follows.

$$T_{direct} = w_{com} \times T_{com} + w_{ene} \times T_{ene} \tag{8}$$

where w_{com} and w_{ene} are weight, and w_{com}+ w_{ene} = 1, w_{com}, w_{ene}∈[0,1].

4.3 Calculation of recommendation trust

When the distance between source and destination nodes is smaller than the communication radius, they can directly transmit data packets. But if the number of interactive packets is not large enough, just considering the direct trust is not enough to reflect the actual situation. In the range of communication radius, we select a set of common neighbors between source and destinations. The neighbors provide recommendation trust aim at destinations to source node. The topological structure of recommendation trust is shown in Fig. 5.

As shown in Fig. 5, Node A is the source, Node B is the destination, and the distance between A and B is smaller than the communication radius. We select a set of common neighbors of source node and destination named C_1,C_2,-C_3,…C_n and the direct trust of node A aim at C_i must be larger than the threshold 0.5. And we can adopt the threshold during different network conditions. C_i provides the recommendation trust aims at B to node A, but not all of the recommendations are reliable. So, we need to evaluate the reliability and familiarity about the recommendation trust (Fig. 6).

4.3.1 Calculation of recommendation reliability

During the calculation of the recommendation trust of nodes, not all of the recommendations are reliable. We need to filter out the malicious and exaggerated recommendations [29]. The formula to calculate the differences between recommendation trusts is as follows.

$$Diff = \frac{|RT_{ave} - RT_i|}{RT_{ave}}$$
$$RT_{ave} = \frac{1}{N} \times \sum_{i=1}^{N} RT_i \tag{9}$$

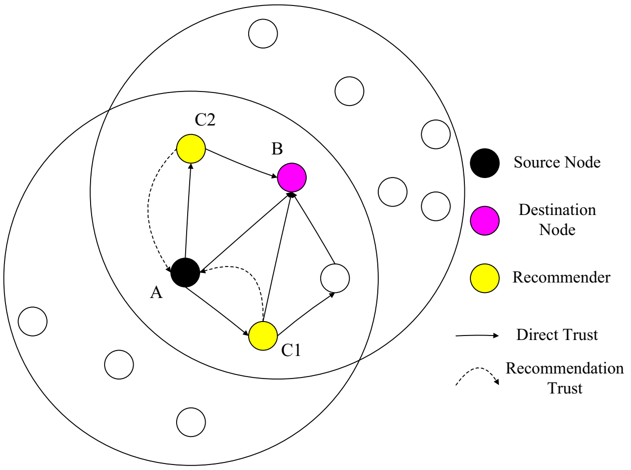


Fig. 5 Topology structure of recommendation trust

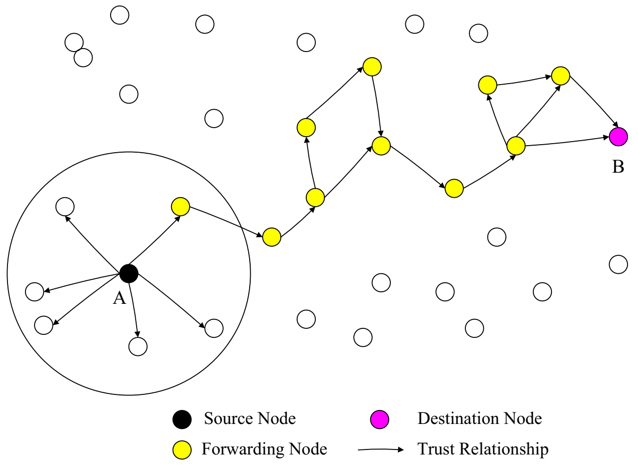


Fig. 6 Topology structure of indirect trust

where RT_i is the recommendation trust of node $\mathrm{C_i}$ aims at node B, N is the number of $\mathrm{C_i}$. RT_{ave} is the average recommendation trust from C_1 to C_n aims at node B. And the value of *Diff* must not be bigger than 1.

According to the above theory, we can get the calculation formula of the recommendation reliability as follows.

$$T_{rel} = 1 - Diff \tag{10}$$

When the source node wants to obtain the effective recommendation trust from the set of common neighbors aim at the destination, we need to calculate the recommendation reliability, and the reliability obeys the above formula with calculation efficiency.

Assume that the distance between node A and B is smaller than the communication radius, and C_i is a set of common neighbors of node A and B. The recommendation trust of C_1, C_2, C_3 aims at node B respectively is 0.3, 0.8 and 0.4. And the average recommendation obtained is (0.3 + 0.8 + 0.4)/3 = 0.5. According to the above formula, the recommendation reliability of C_1 aims at B is 1 − (|0.3–0.5|)/0.5 = 0.6, and the reliability of C_2 aims at B is 1 − (|0.8–0.5|)/0.5 = 0.4, and the reliability of C_3 aims at B is 1 − (|0.4–0.5|)/0.5 = 0.8. According to the above, the reliability of C_3 is the largest. Because of the average recommendation trust is 0.5, and the recommendation trust of C_3 aims at B is 0.4 which is nearest to the average value. Go along with the normal distribution, the more the value is closer to expectation, the higher reliability of the value is. And the effectiveness of method which we propose is verified.

4.3.2 Calculation of recommendation familiarity

Normally, as literature [24] and [30] proposed that the higher the credibility of the source node, the more reliable the recommend-er is and the more reliable recommendation trust is. But that is not the case. Therefore, we introduce the recommendation familiarity. Depending on the times of successful communication between source and destination nodes and the numbers of the common neighbors, we can obtain the formula to calculate the recommendation familiarity as follows.

$$T_{fam} = \frac{Num^B_{C_i}}{Num_{C_i}} \times \frac{m^B_{C_i}}{MC_i} \tag{11}$$

We can count the number of communication packets between nodes. where $Num^B_{C_i}$ is the number of successful communication packets between the recommend-er $\mathrm{C_i}$ and node B. $NumC_i$ is the number of successful communication packets between C_i with other nodes. $\frac{m^B_{C_i}}{MC_i}$ is an adjust factor, as the related degree of B and C_i. m^B_{Ci} is the number of the common neighbors of B and $\mathrm{C_i}$. M_{Ci} is the number of neighbor in one-hop of $\mathrm{C_i}$.

When the source node wants to obtain the effective recommendation trust from the set of common neighbors aim at the destination, we need to calculate the recommendation familiarity, and the familiarity obeys the above formula with calculation efficiency.

Assume that the distance between node A and B is smaller than that of the communication radius, and $\mathrm{C_i}$ is a set of common neighbors of node A and B. The number of communication packets between C_1 and B is 200. The number of communication packets between C_1 and all of the others is 1000. The number of common neighbors of C_1 and B is 4. The number of one-hop neighbors of C_1 is 7. According to the above formula, we can get the recommendation familiarity as (200/1000) × (4/7) = 0.11. To node C_2, the corresponding parameters are 400, 1000, 4 and 7 respectively. We can obtain the recommendation familiarity as (400/1000) × (4/7) = 0.23. To node C_3, the corresponding parameters are 200, 1000, 6 and 7 respectively. We can obtain the recommendation familiarity as (200/1000) × (6/7) = 0.17. To node C_4, the corresponding parameters are 400, 1000, 6 and 7 respectively. We can get the recommendation familiarity as (400/1000) × (6/7) = 0.34. The above analysis shows that, if the number of successful communication packets between $\mathrm{C_i}$ and B is larger, or the number of the common neighbors of $\mathrm{C_i}$ and B is larger, the recommendation trust obtained from the recommenders is much more familiarity. The above analysis shows node C_2 and C_3 have the highest familiarity to node B.

According to the direct trust *TCi* of node A aims at Ci, the direct trust value of $T^B_{C_i}$ of node $\mathrm{C_i}$ aims at B, and the recommendation reliability T_{rel} and familiarity T_{fam}, we can obtain the formula to calculate the recommendation trust as follows.

$$T_{recom} = \frac{\sum_{i=1}^{n} [0.5 + (T_{C_i}^{B} - 0.5) \times T_{rel} \times T_{fam}]}{n} \tag{12}$$

4.4 Calculation of integrate direct trust in one-hop module

By what we discussed above, when the distance between source and destination nodes is smaller than the communication radius, enter into one-hop module. And if the number of communication packets is larger than or equal to the threshold, just calculating the direct trust as integrate direct trust is accurate enough. Otherwise, we need to consider the recommendation trust which obtained from the common neighbors aim at the destination nodes.

In one-hop module, the calculation formula of integrate direct trust is as follows.

$$T(P_i, P_j) = \begin{cases} T_{direct}(P_i, P_j) \quad if & h \geq H \\ w_1 \times T_{direct}(P_i, P_j) + w_2 \times T_{recom}(P, P) \quad if & 0 < h < H \\ 0 \quad if & h = 0 \end{cases} \tag{13}$$

where h is the number of communication packets between source and destination nodes. H is the threshold of communication packets. w_1 and w_2 are weights to adjust the proportion of direct and recommendation trust. The existing methods to set the weight are almost too subjective, such as the expert opinions and average weight method. These methods decrease the scientificity of trust evaluation and lack of flexibility. Once the weights are determined, it is hard to dynamically adjust the value of weight. So, the existing methods to calculate the trust are lack of adaptability.

And we introduce node activeness $\beta(j) \in [0,1]$ which reflects the active degree of nodes in the network. The larger the value of node activeness is, the more of interactive nodes are with this node. That is to say the node has higher credibility.

We set $w_1 = \frac{1}{1+\beta(j)} w_2 = \frac{\beta(j)}{1+\beta(j)}.\beta(j) \in [0, 1]$, so $\frac{1}{1+\beta(j)}$ is not smaller than $\frac{\beta(j)}{1+\beta(j)}$. The weights w_1 and w_2 are automatic calculation based on the systematic mathematics model. The formula to calculate $\beta(j)$ is as follows.

$$\beta(j) = \frac{1}{2} \times \left[\Phi(L_j) + \Phi(n_{total})\right] \tag{14}$$

where L_j is number of the common neighbors between source node and node j. n_{total} is the number of neighbors within the scope of communication radius of node $j.\Phi(x) = 1 - \frac{1}{x+\delta}$, δ is a constant value larger than 0, which used to control the speed of $\Phi(x)$ to tend to 1. From the above formula, the node activeness $\beta(j)$ is decided by L_j and n_{total}. The more the number of interactive node is with j, the larger the value of $\beta(j)$ is.

The Eq. (14) is obtained by us based on our analysis & deduction and relative experiments under different conditions.

Above all, in one-hop module, the calculation formula of integrate direct trust is as follows.

$$T(P_i, P_j) = \begin{cases} T_{direct}(P_i, P_j) \quad if & h \geq H \\ \frac{1}{1+\beta(P_j)} \times T_{direct}(P_i, P_j) + \frac{\beta(P_j)}{1+\beta(P_j)} \times T_{recom}(P_i, P_j) \; if & 0 < h < H \\ 0 \quad if & h = 0 \end{cases} \tag{15}$$

4.5 Calculation of indirect trust in multi-hop module

MANET is a kind of multiple-hop network. When the distance between source and destination nodes is larger than the communication radius, we need to calculate the indirect trust based on the trust propagation. First, we need to obtain the recommenders between source and destination node, namely all of the nodes on the path from source to destination. Second, according to the trust propagation between neighbors on the path, we can calculate the indirect trust between source and destination node.

Among them, we should consider various factors to choose the best nodes to establish the path from the source to the destination node. And the rules to choose nodes are as follows: The node selects the next forwarding node which is the nearest to itself, and the minimum energy consumption during transmit messages; The node selects the next forwarding node which has the maximum residual energy and within the scope of communication radius. That ensures the next forwarding node has enough power to receive and transmit messages; The node selects the next forwarding node which has the maximum integrate direct trust, that is, in order to make the message transmission more reliable.

All of the nodes on the path should propagate the trust. Firstly, the source node sends a message to all its one-hop neighbors, then the neighbors check whether the destination node is its neighbors, besides, the neighbors also check whether there is a path to the destination from itself. If the destination is not the neighbors of itself, then it sends the message to its one-hop neighbors except for the source node, and so on. Once the neighbors of a node contain the destination, the neighbor node would responses to its parent node. And the parent node calculates the indirect trust aims at the destination node based on integrate direct trust to its son node and the recommendation trust achieved from the son node aims at the destination. In this way, until the response message arrives the source node, the source node calculates the indirect trust aims at the destination based on the integrate direct trust to its one-hop neighbor and the indirect trust is obtained from the one-hop neighbor aims at the destination node.

Because of the characteristics of mobility, dynamic topology and so on, we need to consider the distance factor of trust propagation in the network. The calculation formula of the trust propagation distance is as follows.

$$L = \frac{\ln n}{\ln k} \tag{16}$$

where n is the number of nodes in the network, k is the average number of neighbors of each node in the network. We can get the value of n and k according the routing table of each node.

The Eq. (16) is obtained by us based on our analysis & deduction and relative experiments under different conditions.

According to the above, we can get the formula to calculate the indirect trust between nodes as follows.

$$T_{indirect}\binom{B}{C_i+1} = \begin{cases} \frac{\ln n}{\ln k} \times T_{C_i+1}^{C_i} \times T_{indirect}\binom{B}{C_i} & if \quad T_{indirect}\binom{B}{C_i} \le 0.5 \\ \frac{\ln n}{\ln k} \times (0.5 + \left(T_{C_i+1}^{C_i} - 0.5\right) \times T_{indirect}\binom{B}{C_i}) & else \end{cases} \tag{17}$$

$$T_{indirect}\binom{B}{C_2} = \begin{cases} \frac{\ln n}{\ln k} \times T_{C_2}^{C_1} \times T_{C_1}^{B} & if \ T_{C_1}^{B} \le 0.5 \\ \frac{\ln n}{\ln k} \times (0.5 + (T_{C_2}^{C_1} - 0.5)) \times T_{C_1}^{B} & else \end{cases} \tag{18}$$

where $T_{indirect}\binom{B}{C_i+1}$ is the indirect trust of C_{i+1} aims at $B, T_{C_i+1}^{C_i}$ is the integrate direct trust of C_{i+1} aims at C_i,$T_{indirect}\binom{B}{C_i}$ is indirect trust of C_i aims at B. When the message nearly arrives the destination nodes, assume that C_1 is the one-hop neighbor of B, then the indirect trust of the two-hop neighbor C_2 aims at B relies on the integrate direct trust of C_2 aims at C_1 and the recommendation trust of C_1 aims at B.

The Eqs. (17) and (18) are obtained by us based on our analysis & deduction and relative experiments under different conditions.

4.6 Trust update

Because of the characteristics of dynamic topology and self-organizing, the nodes may randomly join in or leave out of the network. So, the trust between nodes should be periodically updated. Firstly, the update should not be too frequent due to the nodes in the shorter period would consume more energy. This is not good for the survival cycle of the network. Secondly, the period of update should not be too long. Because if the update period is too long, the calculated trust value would not accurately reflect the current trust of node. So, we obtain the calculation formula of trust update as follows.

$$T_{n+1} = w_1 \times T_1 + w_2 \times T_2 + \cdots + w_n \times T_n \tag{19}$$

where T_1, T_2, T_3,…T_n respectively represents the history trust value of each node. And we use the IOWA algorithm[31] to calculate the weight w_i, and the algorithm 1 is as follows.

```
Begin
Input($\alpha, \langle t_1, T_D^{(1)}(P_i, P_j)\rangle, \langle t_2, T_D^{(2)}(P_i, P_j)\rangle, \ldots, \langle t_m, T_D^{(3)}(P_i, P_j)\rangle$)
/* For different α and m, we can get different IOWA weight */
/* m is the number of attributes, α is the situation parameter */
n = m;
If $\alpha < 0.5$ then $\alpha = 1 - \alpha$
If $\alpha \ge 0.5$ then {
        $w_1^*[(n-1)\alpha + 1 - nw_1^*]^n = [(n-1)\alpha)^{n-1}[((n-1)\alpha - n)w_1^* + 1]$; /* Calculate $w_1^*$ */
        $w_n^* = \frac{((n-1)\alpha - n)w_1^* + 1}{(n-1)\alpha + 1 - nw_1^*}$;        /* Calculate $w_n^*$ */
For $i = 2$ to $n - 1$ do
        $w_i^* = \sqrt[n-1]{w_1^{*(n-i)} w_n^{*(i-1)}}$        /* Calculate $w_i^*$ */
Output($w_1^*, w_2^*, \ldots w_n^*$)
End
```

According to the above algorithm, the weight coefficients are mainly determined by two parameters: the parameter α and n. n is the round of calculation in the network. α is same as to the learning factor in machine learning algorithms. α reflects the degree of forgetfulness about the history communication behaviors. The more α tends to 1, the more easily can be forgotten about the history behaviors.

4.7 Integrated description of DATEA

According to the above theory and formula, integrated description of the distributed and adaptive trust evaluation algorithm as algorithm 2 is as follows.

1. When the distance between source node and destination node is smaller than or equal to the communication radius, it enters into the one-hop trust module;
   1) When the number of communication packets between source and destination nodes is larger than or equal to the threshold, it is effective enough to just calculate the direct trust. And the direct trust contains communication trust and energy trust;

① Use the formula (3) to calculate the communication trust based on SLF model;

② Use the formula (4) to predict the communication trust based on AR model;

③ Use the formula (5) and (6) to calculate the integrate communication trust based on SLF and AR;

④ Use the formula (1) and (2) according to the energy consumption model to calculate the residual energy of nodes after transmit messages;

⑤ Use the formula (7) to calculate the energy trust;

⑥ Use the formula (8) to calculate the direct trust between nodes, based on the communication trust obtained from step③ and the energy trust obtained from step⑤;

2) When the number of communication packets between source and destination nodes is smaller than the threshold, we need to consider the recommendation trust from the third party;

① Use the formula (9) and (10) to calculate the recommendation reliability;

② Use the formula (11) to calculate the recommendation familiarity;

③ Use the formula (12) to calculate the recommendation trust, based on the recommendation reliability obtained from step① and the recommendation familiarity obtained from step②.

3) Use the formula (13), (14) and (15) to calculate the integrate direct trust in one-hop module, based on the direct trust obtained from step 1) and the recommendation trust obtained from step 2).

2. When the distance between source and destination node is larger than the communication radius, it enters into the multi-hop trust module;

1) Following the rules to select the best forwarding node as the next hop node to transmit messages;

2) Use the formula (16) to calculate the distance of trust propagation;

3) Use the formula (17) and (18) to calculate the indirect trust between nodes;

3. Update the trust

According to the above, step 1) calculates the integrated direct trust in one-hop module, and step 2) calculates the indirect trust in multi-hop module. Use the formula (19) to update the integrated direct trust and the indirect trust. Besides, the algorithm 1 puts out the way to calculate the weights of history trust values.

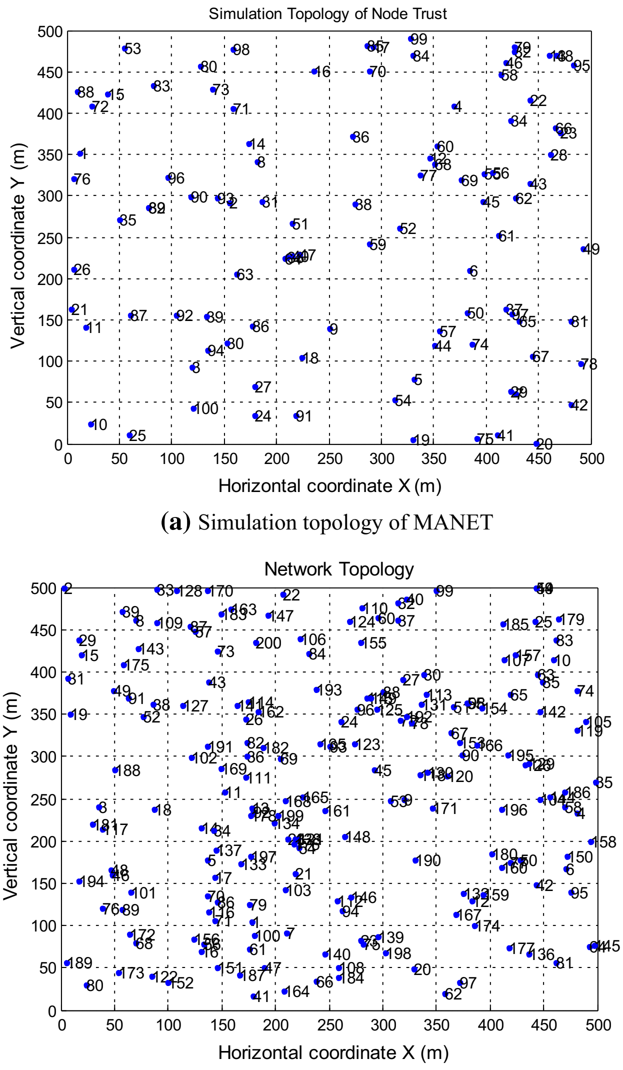
5 Simulation results & analysis

In order to explain the proposed trust calculation can mitigate attacks and show how a malicious node is detected, the detection accuracy, what decision is made with respect to malicious nodes, according to the aforementioned theory and formula, integrated description the distributed and adaptive trust evaluation algorithm, we do many experiments [49–52], which includes the MATLAB simulations and tests of the practical applications of MANET.

Our experimental simulations are performed using MATLAB. First, we evaluate the performance of DATEA in different parameters conditions, like the different threshold of communication packets, different weights, etc. Then, we compare the performance of DATEA, EDTM and NBBTE at the aspects of the detection ratio of malicious nodes and the energy consumption of nodes. The area of network topology is 500 × 500, and randomly distributes 100 nodes. And we adopt three malicious attacks like flooding, select forwarding attacks and bad/good-mouthing attacks. The network topology of MANET is shown in Fig. 7a. We introduce the calculation of trust value under the ideal state. Under the ideal conditions, the nodes are without moving, the network is without malicious nodes and interference like network latency, etc (Table 1).

In Figs. 8 and 9, (a) is the trust of normal nodes under the ideal condition; (b) is the direct trust of normal nodes under common condition; (c) is the integrate direct trust of normal nodes in one-hop module under the common condition; (d) is the trust of malicious nodes under the ideal condition; (e) is the direct trust of malicious nodes under common condition; (f) is the integrate direct trust of malicious nodes in one-hop module under the common condition.

As shown in Fig. 8. Under the ideal state, the network is without any malicious attacks such as interference, so the trust of normal nodes remains for the initial value 1, and the trust of malicious nodes decreases continually. Under the normal condition, due to the effects like delay, network congestion and malicious attacks and so on, the trust of nodes cannot perform best. It can be seen from Fig. 8,



(a) Simulation topology of MANET

(b) The topology of practical application

Fig. 7 Network topology of MANE for experiments

Table 1 Simulation parameters

Area of network topology	500(m) × 500(m)
Total number of nodes *NodeNums*	100
Communication radius	100 (m)
Length of data packets	2000bit
Threshold of communication distance d_0	87
Initial trust of nodes	1
Initial energy of nodes	0.9 J
Coefficient of circuit energy consumption	5.0 × 10–8 J/bit
Coefficient of energy channel propagation model	ε_{fs}:1.0 × 10–11 J (bit·m-2) ε_{mp}:1.3 × 10–15 J/(bit·m-4)
Threshold of trust that source aims at recommenders	0.5

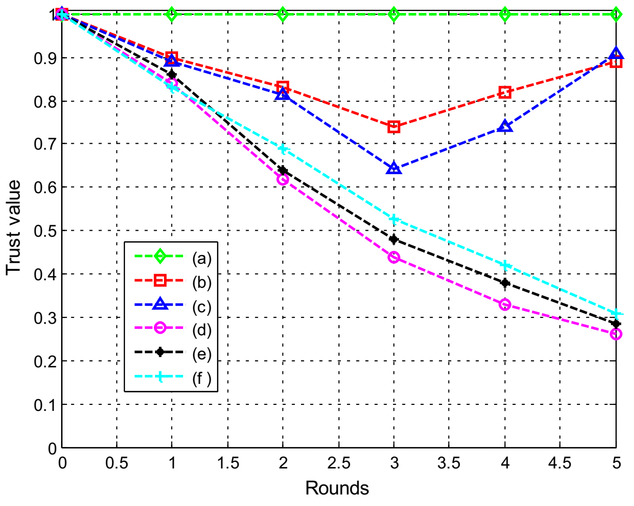


Fig. 8 Trust of nodes when the number of communication packets is larger than the threshold

when the number of communication packets is larger than the threshold, the direct trust of normal nodes is closer to the ideal state and better than the integrated direct trust. The graph is decline first and then rise. That is because each node sends packets to the links in the initial state, which leads to link congestion and the lower packet submit rate. And the communication trust between nodes becomes lower. With the stable of network, the nodes enter into the state of listening, sending and receiving orderly. The trust of nodes is rising. But to malicious nodes, we can find that when the number of communication packets is larger than the threshold, the calculated direct trust is closer to the ideal value, and keeps the trend of decline.

As shown in Fig. 9. When the number of communication packets is smaller than the threshold, under the ideal state, the network is without any interference, so the trust of normal nodes remains to the initial value 1, and the trust of malicious nodes decreases continually. We can find that the integrated direct trust of normal nodes is closer than the ideal state and better than the direct trust in one-hop module. To malicious nodes, we can find that the calculated integrate direct trust is closer to the ideal value, and keeps the trend of decline.

Figure 10 shows the relationship between the trust of normal nodes, the number of communication packets and the threshold of communication packets. (a) is the trust of nodes when the threshold is 20% of the number of communication packets. (b) is the trust of nodes when the threshold is 40%. (c) is the trust of nodes when the threshold is 60%. (d) is the trust of nodes when the threshold is 80%. When the number of communication packets is lower than 250, the trust under the condition of threshold 40% performs best and closer to the ideal state. When the number of packets is larger than 250 and smaller

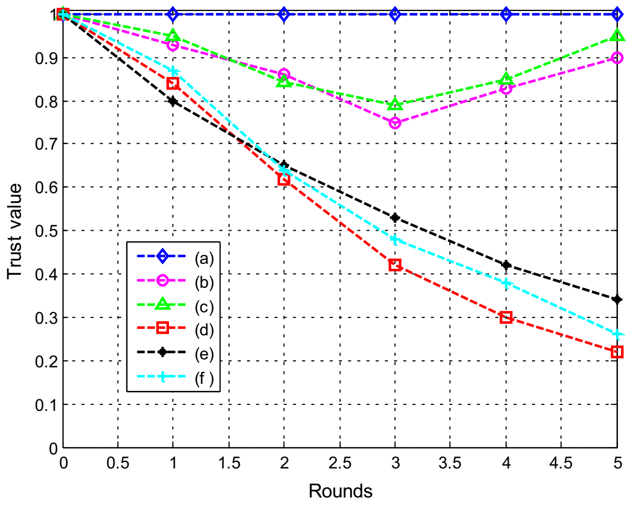


Fig. 9 Trust of nodes when the number of communication packets is smaller than the threshold

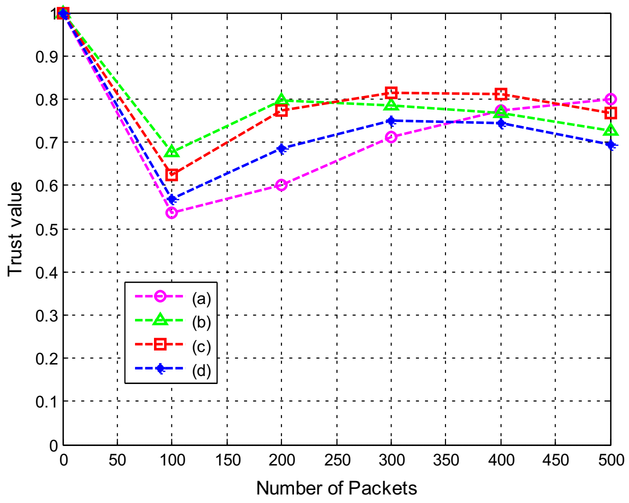


Fig. 10 Relationship between trust and numbers of communication packets

than 450, the trust under the condition of threshold 60% performs best. When the packets is larger than 450, the trust under the condition of threshold 20% performs best. So, we can adjust the threshold value according to different network conditions.

In the one-hop module, the integrated direct trust is depended on the direct and the recommendation trust. As shown in Fig. 11, we adaptively adjust the weight to calculate the trust value. There is a certain proportion of malicious nodes in the network. Compare the adaptive weighting in DATEA with manual set the weight, we can get that, when the malicious nodes are less than 5%, the weight of (0.2, 0.8) performs best. With the increase of proportion of malicious nodes, the adaptive weight by using DATEA performs better than others.

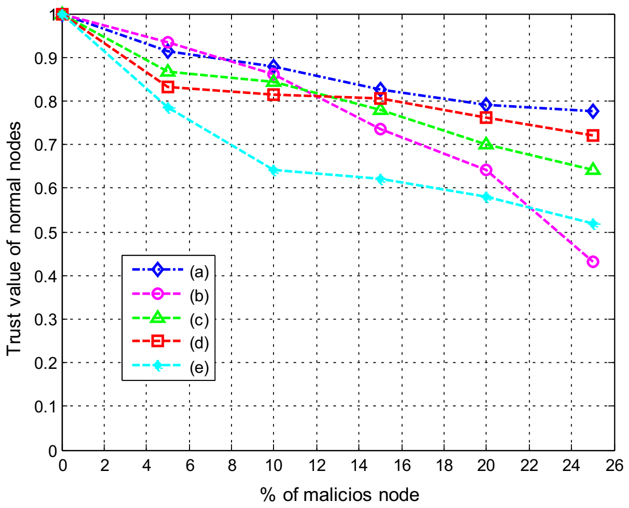


Fig. 11 Relationship between integrate direct trust and the coefficient weight in one-hop module

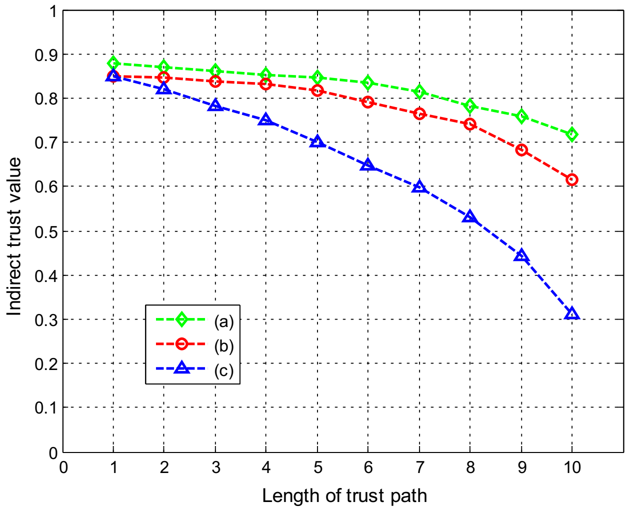


Fig. 12 Comparison of indirect trust between nodes

In Fig. 11, (a) is the adaptive weighting of DATEA. (b) is the weight of (0.2,0.8). (c) is the weight of (0.4,0.6). (d) is the weight of (0.6,0.4). (e) is the weight of (0.8,0.2).

In Figs. 12 and 13, (a) is DATEA, (b) is EDTM, (c) is NBBTE.

As shown in Fig. 12, we compare the indirect trust by using three different methods. For example, the trust of nodes is 0.7 under the ideal state, and the direct trust from its one-hop neighbor is 0.7, the indirect trust from its two-hop neighbor is 0.6. According to NBBTE, we can obtain that the indirect trust from its three-hop neighbor is $0.6 \times 0.6 \times 0.7 = 0.294$. In EDTM, we can get the trust value as $0.5 + (0.6 - 0.5) \times (0.5 + (0.7 - 0.5) \times 0.7) = 0.564$. Based on DATEA, we can get the trust value as (ln100/

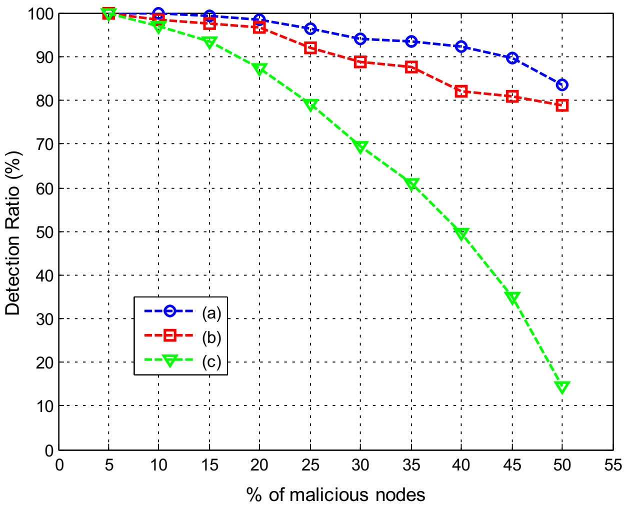


Fig. 13 Comparison of detection rate of malicious nodes

ln14) × 0.5 + (0.6 − 0.5) × (0.5 + (0.7 − 0.5) × 0.7) = 0.581. And 0294 < 0.564 < 0.581 < 0.7, so we can find that the DATEA performs best which is nearest to the ideal state.

In order to explain how the malicious nodes are simulated, they perform any real attack by good/bad-mouthing nodes, selectively forwarding packets or flooding the network and the implemented method, according to the aforementioned theory and formula, DATEA algorithm, we do many experimental tests of the practical applications of MANET. The MANET structure of our experimental tests of the practical application is as Fig. 1 with simple structure, Fig. 2 with Multi-hop network and Fig. 7b with practical application topology of MANET.

The feature of the proposed method is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. During the implemented process, we focus on the detection phase and present different kinds of sensors that can be used to find selfish nodes. The detection process of our method is called activity-based overhearing, iterative probing, and unambiguous probing. Our proposed trust calculation attempts to resolve the relative issue by designing a dynamic source routing mechanism, which is referred to as the cooperative bait detection scheme, that integrates the advantages of both proactive and reactive defense architectures. Our method implements a reverse tracing technique to help in achieving the stated goal.

As shown in Fig. 13, we set a percentage of the malicious nodes in the network, by using these three methods to detect malicious nodes, compare the detection rate with each other. In the experiments of the practical application of MANET, we adopt the flooding, selective forwarding attacks and the bad/good-mouthing attacks. The Fig. 13 shows that DATEA performs better than NBBTE and EDTM. Because of NBBTE is just effective of detect the selective forwarding attacks, and EDTM is effective in the detection of selective forwarding and bad/good-mouthing attacks. But when the number of packets is large enough, due to the non-adaptive of weight coefficient among direct trust and indirect trust in EDTM, the calculated trust is largely different with the actual value. From Fig. 13, we can find that the DATEA has a better robustness to against these attacks.

As shown in Fig. 14. We set a proportion of malicious nodes with flooding and selective forwarding attacks. Compare the robustness of different methods and the detection rate of malicious nodes. And (a) is DATEA faced with selective forwarding, (b) is EDTM faced with selective forwarding, (c) is NBBTE faced with selective forwarding, (d) is DATEA faced with flooding, (e) is EDTM faced with flooding, (f) is NBBTE faced with flooding. From Fig. 14, we can conclude that DATEA and EDTM have a nice performance faced with selective forwarding. But when it comes to flooding, the DATEA performs better than the two others due to the adaptive weight. Figure 14 shows that DATEA performs better than EDTM and NBBTE.

As shown in Fig. 15, (a) is DATEA, (b) is EDTM, (c) is NBBTE. We know that detecting the malicious nodes will consume energy of nodes. Calculate the residual energy of all nodes in the network during the detection rate reaches a certain proportion. From Fig. 15, we can find that when the detection rate is smaller than 35%, DATEA has a better performance than the two others. But with the increasing of detection rate, the energy consumption of DATEA is larger than EDTM. That is because EDTM keeps only the information of one-hop neighbors. But in DATEA, to calculate the indirect trust, the nodes need to keep all

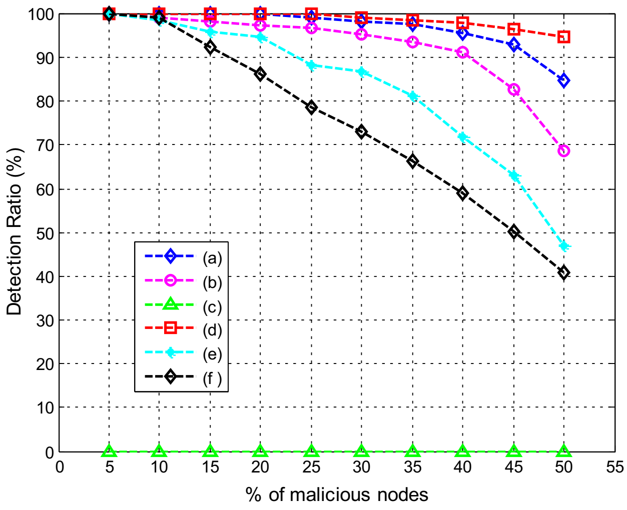


Fig. 14 Comparison of the robustness against certain attacks

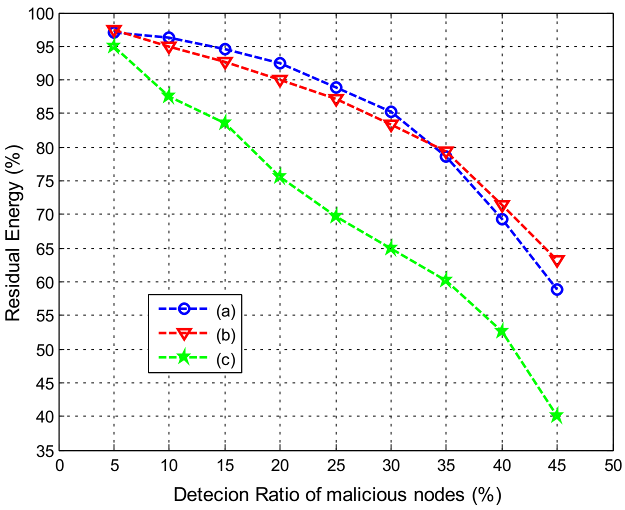


Fig. 15 Comparison of energy consumption

information of nodes in the trust propagation path. The more information is stored, the more energy the nodes consumes. Thankfully, DATEA mainly considers the reliability of data transmission. The DATEA is suit for MANET and different from EDTM in WSN. The nodes like phones could be battery charging, so the DATEA is not very urgent in energy consumption.

6 Conclusions

We propose a novel approach of distributed & adaptive trust metrics for MANET (DATEA) in this paper. In DATEA, we define the one-hop module and multi-hop module. The one-hop module contains the calculation of direct trust and recommendation trust, and the multi-hop module contains the calculation of indirect trust. The direct trust includes communication trust and energy trust. When we calculate the communication trust, not only consider the current value, but also predict it according to the state of network. The method adaptively sets the weights in one-hop module, and calculates the integrate trust both considering the direct and recommendation trust. In the calculation of indirect trust, we consider not only direct and recommendation trust, but also the propagation distance of trust. And the trust updated method is discussed in this paper. Our experiments and tests of the practical applications of MANET show that the DATEA performs better than that of EDTM and NBBTE at the aspects of evaluate node trust and detect the malicious in the network.

Acknowledgement This research work is supported by National Natural Science Foundation of China (Grant No. 61571328), Tianjin Key Natural Science Foundation (No.18JCZDJC96800), CSC Foundation (No. 201308120010), Major projects of science and technology in Tianjin (No.15ZXDSGX 00050), Training plan of Tianjin University Innovation Team (No.TD12-5016, TD13-5025), Major projects of science and technology for their services in Tianjin (No.16ZXFWGX00010, No.17YFZC GX00360), the Key Subject Foundation of Tianjin (No.15JC YBJC46500), Training plan of Tianjin 131 Innovation Talent Team (No.TD2015-23).

References

1. Zhang, D. G., Li, G., & Zheng, K. (2014). An energy-balanced routing method based on forward-aware factor for wireless sensor network. *IEEE Transactions on Industrial Informatics, 10,* 766–773.
2. Tan, S. S., Li, X. P., & Dong, Q. K. (2015). Trust based routing mechanism for securing OLSR-Based MANET. *Ad Hoc Networks, 30,* 84–98.
3. Gungor, V. C., Bin, L., & Hancke, G. P. (2010). Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Transactions on Industrial Electronics, 57*(10), 3557–3564.
4. Chen, J. Q., & Mao, G. Q. (2018). Capacity of cooperative vehicular networks with infrastructure support: Multi-user case. *IEEE Transactions on Vehicular Technology, 67*(2), 1546–1560.
5. Wang, X., Liu, L., & Su, J. (2012). RLM: A general model for trust representation and aggregation. *IEEE Transactions on Services Computing, 5,* 131–143.
6. Song, X. D., & Wang, X. (2015). Extended AODV routing method based on distributed minimum transmission (DMT) for WSN. *International Journal of Electronics and Communications, 69*(1), 371–381.
7. Wang, X. (2017). A kind of novel VPF-based energy-balanced routing strategy for wireless mesh network. *International Journal of Communication Systems, 30*(6), 1–15.
8. Zhang, D. G. (2012). A new approach and system for attentive mobile learning based on seamless migration. *Applied Intelligence, 36,* 75–89.
9. Niu, H. L. (2017). Novel positioning service computing method for WSN. *Wireless Personal Communications, 92*(4), 1747–1769.
10. Zhang, D. G., & Zhu, Y. N. (2012). A new constructing approach for a weighted topology of wireless sensor networks based on local-world theory for the internet of things (IOT). *Computers & Mathematics with Applications, 64,* 1044–1055.
11. Artz, D., & Gil, Y. (2007). A survey of trust in computer science and the semantic web. *Web Semantics, 5,* 58–71.
12. Shao, K., & Luo, F. (2012). Normal distribution based dynamical recommendation trust model. *Journal of Software, 23*(12), 3130–3148.
13. Govindan, K., & Mohapatra, P. (2012). Trust computations and trust dynamics in mobile ad hoc networks: A survey. *IEEE Communications Surveys & Tutorials, 14*(2), 279–298.
14. Nordheimer, K., & Schulze, T. (2010). Trustworthiness in networks: A simulation approach for approximating local trust and distrust values. *IEEE Communications Surveys and Tutorials, 321,* 157–171.
15. Hsieh, M. Y., Huang, Y. M., & Chao, H. C. (2007). Adaptive security design with malicious node detection in cluster-based sensor networks. *Computer Communications, 30,* 2385–2400.
16. Li, W. B. (2016). Novel ID-based anti-collision approach for RFID. *Enterprise Information Systems, 10*(7), 771–789.
17. Safa, H., Artail, H., & Tabet, D. (2010). A cluster-based trust-aware routing protocol for mobile ad hoc networks. *Wireless Networks, 16,* 969–984.
18. Li, L., Fan, L., & Hui, H. (2009). Behavior-driven role-based trust management. *Journal of Software, 20,* 2298–2306.
19. Cho, J. H., Swami, A., & Chen, I. R. (2012). Modeling and analysis of trust management with trust chain optimization in

mobile ad hoc networks. *Journal of Network and Computer Applications, 35,* 1001–1012.
20. Li, N. H., & Mitchell, J. C. (2005). Beyond proof-of- compliance: Security analysis in trust management. *Journal of the ACM, 52,* 474–514.
21. Wang, X., & Song, X. D. (2015). New medical image fusion approach with coding based on SCD in wireless sensor network. *Journal of Electrical Engineering & Technology, 10*(6), 2384–2392.
22. Niu, H. L. (2017). Novel PEECR-based clustering routing approach. *Soft Computing, 21*(24), 7313–7323.
23. Feng, R. J., Xu, X. F., & Zhou, X. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory. *Sensors, 11,* 1345–1360.
24. Jiang, J. F., Han, G. J., & Wang, F. (2015). An efficient distrubuted trust model for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 26,* 1228–1237.
25. Zhou, S., & Chen, J. (2017). New Dv-distance method based on path for wireless sensor network. *Intelligent Automation and Soft Computing, 23*(2), 219–225.
26. Zhang, T. (2018). Novel optimized link state routing protocol based on quantum genetic strategy for mobile learning. *Journal of Network and Computer Applications, 2018*(122), 37–49.
27. Li, G., & Pan, Z. H. (2014). A new anti-collision algorithm for RFID tag. *International Journal of Communication Systems, 27*(11), 3312–3322.
28. Chatterjee, P., & Sengupta, I. (2014). A trust enhanced secure clustering framework for wireless ad hoc networks. *Wireless Networks, 20,* 1669–1684.
29. Wang, G., & Gui, X. L. (2013). The selection of trading node and the calculation method of trust relationship in social network. *Chinese Journal of Computers, 36,* 368–383. **(in Chinese with English abstract)**.
30. Zhu, Y. N., Liu, S., & Zhang, X. D. (2016). Multi-radio multichannel (MRMC) resource optimization method for wireless mesh network. *Journal of Information Science and Engineering, 32*(2), 501–519.
31. Li, X. Y., & Gui, X. L. (2010). The cognitive model of dynamic trust. *Journal of Software, 21,* 163–176. **(in Chinese with English abstract)**.
32. Yuan, W. W., Guan, D. H., & Lee, Y. K. (2010). The small-world trust network. *Appliede Intelligence, 35,* 399–410.
33. Liu, S. (2017). Novel unequal clustering routing protocol considering energy balancing based on network partition & distance for mobile education. *Journal of Network and Computer Applications, 88*(15), 1–9. https://doi.org/10.1016/j.jnca.2017.03.025.
34. Ma, Z. (2016). A novel compressive sensing method based on SVD sparse random measurement matrix in wireless sensor network. *Engineering Computations, 33*(8), 2448–2462.
35. Zhang, X. D. (2012). Design and implementation of embedded un-interruptible power supply system (EUPSS) for web-based mobile application. *Enterprise Information Systems, 6*(4), 473–489.
36. Tang, Y. M. (2018). Novel reliable routing method for engineering of internet of vehicles based on graph theory. *Engineering Computations*. https://doi.org/10.1108/ec-07-2018-0299.
37. Zhao, C. P. (2012). A new medium access control protocol based on perceived data reliability and spatial correlation in wireless sensor network. *Computers & Electrical Engineering, 38*(3), 694–702.
38. Liang, Y. P. (2013). A kind of novel method of service-aware computing for uncertain mobile applications. *Mathematical and Computer Modelling, 57*(3–4), 344–356.
39. Ma, Z. (2017). Shadow detection of moving objects based on multisource information in internet of things. *Journal of Experimental & Theoretical Artificial Intelligence, 29*(3), 649–661.
40. Kang, X. J. (2012). A novel image de-noising method based on spherical coordinates system [J]. *EURASIP Journal on Advances in Signal Processing, 2012*(110), 1–10. https://doi.org/10.1186/1687-6180-2012-110.
41. Zhang, D. G. (2014). A novel approach to mapped correlation of ID for RFID anti-collision. *IEEE Transactions on Services Computing, 7*(4), 741–748.
42. Liu, S., & Liu, X. H. (2018). Novel dynamic source routing protocol (DSR) based on genetic algorithm-bacterial foraging optimization (GA-BFO). *International Journal of Communication Systems, 31*(18), 1–20. https://doi.org/10.1002/dac.3824.
43. Song, X. D. (2015). New agent-based proactive migration method and system for big data environment (BDE). *Engineering Computations, 32*(8), 2443–2466.
44. Chen, C., & Cui, Y. Y. (2018). New method of energy efficient subcarrier allocation based on evolutionary game theory. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-018-1123-y.
45. Wang, X. (2015). New clustering routing method based on PECE for WSN. *EURASIP Journal on Wireless Communications and Networking, 2015*(162), 1–13. https://doi.org/10.1186/s13638-015-0399-x.
46. Zheng, K. (2016). Novel quick start (QS) method for optimization of TCP. *Wireless Networks, 22*(1), 211–222.
47. Zheng, K. (2015). A novel multicast routing method with minimum transmission for WSN of cloud computing service. *Soft Computing, 19*(7), 1817–1827.
48. Zhang, D. G., & Ge, H. (2018). New multi-hop clustering algorithm for vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/tits.2018.2853165.
49. Zhou, S., & Tang, Y. M. (2018). A low duty cycle efficient MAC protocol based on self-adaption and predictive strategy. *Mobile Networks and Applications, 23*(4), 828–8392. https://doi.org/10.1007/s11036-017-0878-x.
50. Zhang, T., & Zhang, J. (2018). A kind of effective data aggregating method based on compressive sensing for wireless sensor network. *EURASIP Journal on Wireless Communications and Networking, 2018*(159), 1–15. https://doi.org/10.1186/s13638-018-1176-4.
51. Zhao, D. X., Ma, Z., & Zhang, D. G. (2016). A distributed and adaptive trust evaluation algorithm for MANET. *ACM MSWiM/Q2SWinet'16, 11,* 47–54.
52. Zhang, T. (2018). Novel self-adaptive routing service algorithm for application of VANET. *Applied Intelligence, 11,* 1–5. https://doi.org/10.1007/s10489-018-1368-y.

De-gan Zhang (M'01) Born in 1969, Ph.D, a Member (M) of IEEE in 2001. Graduated from Northeastern University, China. Now he is a professor of Tianjin Key Lab of Intelligent Computing and Novel software Technology, Key Lab of Computer Vision and System, Ministry of Education, Tianjin University of Technology, Tianjin, 300384, China. His research interest includes ITS, WSN, IOT, etc.

Jin-xin Gao (M'16) Born in 1994, Ph.D candidate, a Member (M) of IEEE in 2016. Now she is a researcher Tianjin University of Technology, Tianjin, 300384, China. Her research interest includes WSN, industrial application, etc.

Xiao-huan Liu (M'15) Born in 1989, Ph.D candidate, a Member (M) of IEEE in 2015. Now she is a researcher Tianjin University of Technology, Tianjin, 300384, China. Her research interest includes ITS, WSN, etc.

Ting Zhang (M'05) Born in 1972, Ph.D, a Member (M) of IEEE in 2005. Now she is a researcher of Tianjin Key Lab of Intelligent Computing and Novel software Technology, Key Lab of Computer Vision and System, Ministry of Education, Tianjin University of Technology, Tianjin, 300384, China. Her research interest includes ITS, WSN, etc.

De-xin Zhao (M'05) Born in 1973, Ph.D. a Member (M) of IEEE in 2005. Now she is a professor of Tianjin University of Technology, Tianjin, 300384, China. His research interest includes WSN, mobile computing, etc.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.