IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 January 2023, accepted 9 February 2023, date of publication 14 February 2023, date of current version 22 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3244933

TOPICAL REVIEW

Trust Evaluation and Decision Based on D-S Evidence Theory: Early Models and Future Perspectives

WUXIONG ZHANG[1,2,3], (Member, IEEE), HAOHUI SUN[1,2], WEIDONG FANG[1,2,3], (Member, IEEE), CHUNSHENG ZHU[4], (Member, IEEE), AND GUOQING JIA[5]

[1]Science and Technology on Microsystem Laboratory, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 201899, China
[2]University of Chinese Academy of Sciences, Beijing 100049, China
[3]Shanghai Research and Development Center for Micro-Nano Electronics, Shanghai 201210, China
[4]College of Big Data and Internet, Shenzhen Technology University, Shenzhen, Guangdong 518118, China
[5]College of Physics and Electronic Information Engineering, Qinghai Minzu University, Xining 810007, China

Corresponding author: Weidong Fang (weidong.fang@mail.sim.ac.cn)

This work was supported in part by the Shanghai Natural Science Foundation under Grant 21ZR1461700, and in part by the Special Projects for Key Research and Development Tasks in the Autonomous Region under Grant 2022B01009.

ABSTRACT Due to the technical characteristics and application scenarios of distributed networks, their nodes can easily be invaded and compromised. It will result in information being forged or tampered without difficulty. An effective scheme to guarantee the authenticity and integrity of information is judging how trustworthy nodes are in terms of transmission. In D-S evidence theory (DST), the uncertainty can be expressed to solve the trust fusion issue for multiple nodes. In this paper, for reviewing the DST-based trust evaluation and decision and providing their future research directions systematically. Meanwhile, the DST is briefly reviewed, and two improvements in DST are categorically described. The role and mechanism in DST-based trust models are compared and analyzed. The valuable research directions in the near future are represented. Our contributions could solve the trust problem in resource constrained sensor nodes and improve the decision reliability of network.

INDEX TERMS D-S evidence theory, distributed network, trust model.

I. INTRODUCTION

With the development of social requires and technology, distributed networks are gradually replacing centralized networks. Decentralization and heterogeneity are the trend of future networks [1]. Usually, a centralized network requires a central node to storage, manage, analyze, and process all terminal information in this area. The over-centralized access nodes are at risk of failure [2]. If the central node is compromised or attacked, the network will lose the ability to exchange data. Meanwhile, since all core programs are in the central node, its performance requirements become higher and higher with the more connected objects. Unlike the centralized network, a transmission path can be re-established through other nodes to complete the information transmission in a distributed network, when a relay node in the original path is destroyed or compromised.

The nature of the distributed network makes nodes vulnerable to security attacks, which involving external attacks and internal attacks. The existing cryptography-based security schemes are able to detect malicious behavior from external attacks, while not effective to defend internal attacks [3]. The trust model is widely considered as one of the effective schemes to detect internal attacks and identify compromised nodes. The effective trust evaluation and decision can facilitate to establish secure routing protocols for trusted transmission [4], [5], [6].

How to build trust models efficiently and accurately is a complex multidimensional aggregation problem. The uncertainty of trust factors (e.g., reputation, time weights,

The associate editor coordinating the review of this manuscript and approving it for publication was Hongwei Du.

third-party recommendations, etc.) makes trust evaluation more subjective. DST can express the concept of uncertainty and quantify trust factors to obtain trust between nodes. Feng et al. got direct trust by evaluating the trust degree between nodes through trust factors, and indirect trust was calculated by a trust chain consisting of multi-hop nodes [7]. When fusing information, the D-S combination rule can fuse the uncertainty of multiple sensor nodes. Compared with other schemes, the determination scan be made to have better results and improve the detection capability of the system. Tian et al. [8] computed and analyzed the trust degree of all sensor nodes at the fusion decision layer to improve the anti-attack capability of WSN.

Because DST can solve the problem of uncertainty in trust evaluation and decision and improve the reliability and robustness of the whole network, DST-based trust models are becoming an interesting research hot spot. However, there is seldom paper to analyze and summarize these approaches systematically, in order to facilitate understand DST-based trust, the relationship between them, and how to construct or optimize trust models by adopting DST. The contributions of this review are summarized as follows:

1) Two improvement schemes of DST are summarized, including modification of combination rules and preprocessing of evidence. The role of DST is analyzed in distributed networks.

2) A systematic overview of existing trust models is presented from trust evaluation and decision. The differences between the models are compared when using trust factors. Meanwhile, the trust models are summarized from the perspective of improving DST.

3) Future research directions in DST-based trust models are proposed, including auto-exclusion of malicious nodes, low computational complexity, and emotion-based trust factors to further improve trust management schemes.

The rest of this article is organized as follows. Section II briefly describes the DST and its use in trust models. Section III summarizes and analyzes the existing trust schemes. Section IV proposes some ideas for future work. Finally, a summary is presented in Section V.

II. D-S EVIDENCE THEORY AND DEVELOPMENTS

A. D-S EVIDENCE THEORY

Evidence theory was proposed by Dempster in 1967. On this basis, Shafer used the belief function to expand the evidence theory. After explaining the upper and lower bound of probabilities, he perfected the evidence theory and named it as the Dempster-Shafer theory [9]. In Fig. 1 the relationship between the definitions in DST is described.

Definition 1: Frame of Discernment (FOD)

The frame of discernment is the foundation of the DST. It consists of N mutually exclusive hypotheses. The FOD is defined as:

$$\Theta = \{E_1, E_2, E_3, \ldots, E_N\}. \tag{1}$$

The power set of the FOD is expressed by:

$$2^{\Theta} = \{\phi, \{E_1\}, \ldots, \{E_N\}, \ldots, \{E_1, E_2, \ldots, E_i\}, \ldots, \Theta\}. \tag{2}$$

Definition 2: Basic Probability Assignment (BPA)

Supposing Θ is a FOD, FOD assigns a belief to each element of the power set 2^{Θ}. Supposing A is a subset in Θ, the mapping is:

$$m : 2^{\Theta} \to [0, 1]. \tag{3}$$

which satisfies the following conditions:

$$\begin{aligned} m(\emptyset) &= 0 \\ m(A) &\geq 0 \\ \sum_{A \in 2^{\Theta}} m(A) &= 1. \end{aligned} \tag{4}$$

M is called a basic probability assignment under Θ. It is also called mass function. The mass function indicates the degree of support of the evidence for A.

Definition 3: Belief Function (Bel)

The belief function is defined as the sum of all masses of subsets.

$$Bel(A) = \sum\nolimits_{B \subseteq A} m(B), A \subseteq \Theta. \tag{5}$$

Belief function indicates the trust degree that A is true. But it cannot indicate the trust degree that A is not false. So, the plausibility function is introduced.

Definition 4: Plausibility Function (Pl)

The plausibility function is defined as the sum of all masses of the sets B intersected by set A:

$$Pl(A) = \sum\nolimits_{B \cap A \neq \phi} m(B) = 1 - Bel\left(\bar{A}\right), A \subseteq \Theta. \tag{6}$$

So, the upper and lower bounds of the probability interval can be defined by $[Bel(A)\ Pl(A)]$ to express the uncertainty of evidence.

Definition 5: Dempster-Shafer Combination Rule

If m_1 and m_2 are two independent mass functions defined on Θ, and $A, B, C \subseteq \Theta$, the dempster combination rule is defined as:

$$\begin{aligned} m(A) &= \begin{cases} \dfrac{\sum\limits_{B \cap C = A} m_1(B) \cdot m_2(C)}{1 - k}, & A \neq \emptyset \\ 0, & A = \emptyset \end{cases} \\ k &= \sum_{B \cap C = \phi} m_1(B) \cdot m_2(C). \end{aligned} \tag{7}$$

where, k is a conflict factor and $0 < k < 1$. It used to measure the degree of conflict between and. When $k = 1$ means m_1 and m_2 are full conflict.

At present, in DST, there are still many challenges:

1) it may produce counterintuitive results, when the conflict between the evidence is too high.

2) it is difficult to realize mutually independent assumptions in practical application scenarios.

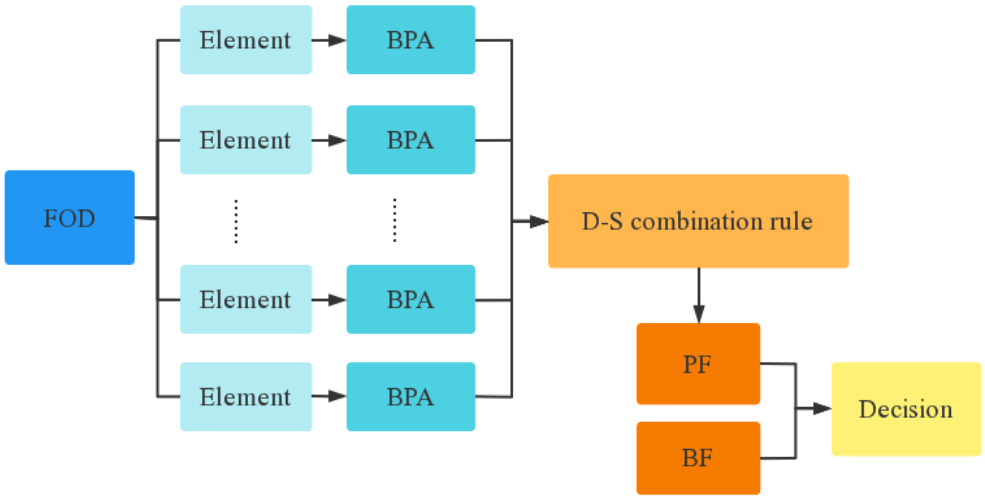


FIGURE 1. Relationship between DST.

3) Dempster combination rule has a high computation complexity. With the development of the elements in FOD, the number of events and computation complexity will grow exponentially.

In the trust management of distributed network, the topology of the network is easy to change because of the mobility of the nodes. When the node position changed, the trust between nodes will change accordingly. Therefore, the exchange and combination laws in D-S combination rules are critical for distributed networks.

Most of schemes for preprocessing evidence in distributed networks are focusing on the similarity degree and solve high conflicts between evidence by similarity weights. However, many existing experiments have shown that improving the entropy will give better results when preprocessing evidence. Meanwhile, the complex evidence theory has proved that the more node information can be recorded to improve the accuracy of node trust. Therefore, in this review, we conclude the schemes of modifying the D-S combination rule and preprocessing evidence to improve the role of DST in trust management.

1) MODIFYING D-S COMBINATION RULE

In existing research, modifying D-S combination rule to address the high conflict between evidence is a common approach. But some schemes may cause the D-S combination rule to lose the mathematical properties of the exchange and combination laws. Combined with the summary of Zhao et al. [10] and Ma et a. [11], The schemes of modifying the combination rules are summarized as shown in Table 1.

2) PREPROCESSING EVIDENCE

It is also common to preprocess evidence before combining multiple pieces of evidence using the D-S rule. Preprocessing evidence can not only solve the problem of conflict between evidences, but also avoid the problems of modifying combination rules such as loss of exchange laws and combination laws.

Current schemes for preprocessing evidence mainly include modifying entropy, divergence and distance between evidence However, the influence mechanisms of evidence in practical applications are often more complex. Therefore, considering more evidence information will improve the accuracy and robustness of evidence fusion. Xiao [15], [16] and Pan and Deng [17] extended the DST to the complex form and added phase information in traditional DST, in order to better record the information of sensor nodes and improve the accuracy of data fusion. Combined with the summary of entropy by Deng [18], the schemes of preprocessing evidence are re-summarized as shown in Table 2.

B. DST-BASED TRUST

For distributed networks, the information collected by a single sensor node is generally incomplete and inaccurate. It needs to collect information from multiple sensor nodes to make judgments about an event. However, the nodes can easily be compromised to become malicious nodes and send false information. It is necessary to judge whether the nodes are trusted to ensure the accuracy of the information. The introduction of DST can construct a more efficient trust model and guarantee the trusted transmission of information.

In DST-based trust, after collecting the information from the nodes, the trust degree of nodes in distributed network is expressed by the elements of FOD to solve the difficulty of representing uncertainty. By preprocessing nodes' data, it reassigns the BPAs of their trust degree weights to avoid too much or too little trust in individual nodes, and improve the availability of data. Meanwhile, D-S combination rule can combine multiple trusts and output an integrated trust with higher trust degree to judge whether the target node is trusted, and avoid the node being invaded to send error messages.

Most of the existing trust models use ternary trust (trust, distrust, and uncertainty) or five elements of trust combined

TABLE 1. Schemes of modifying the D-S combination rule.

Schemes	Key ideas	Exchange and combination laws
Yager [12]	Modified the conflict factor and divided the conflict factor to the set containing all hypotheses.	✓
Dubois [13]	It can be degraded to Yager's method and make a trade-off between reliability and accuracy.	×
Murphy [14]	Averaging the BPA over n pieces of evidence and iterating n-1 times by D-S combination rule.	×
Ma [11]	Reallocating conflicting evidence based on similarity between evidences. But only for full conflict cases.	✓
Xiao [15]	Extending the D-S combination rule to the complex form.	✓

TABLE 2. Schemes of preprocessing evidence.

Schemes	Formula	Key ideas
Yager [19]	$H_Y(m) = -\sum_{A\in X} m(A)\log_2 Pl(A)$	Entropy
Dubois [20]	$l_{DP}(m) = \sum_{A\in X} m(A)\log_2 \lvert A\rvert$	Entropy
Deng [21]	$H_{DE}(m) = -\sum_{A\in 2^\Theta} m(A)\log\left(\frac{m(A)}{2^{\lvert A\rvert}-1}\right)$	Entropy
Cui [22]	$E(m) = -\sum_{A\subseteq X} m(A)\log_2\left(\frac{m(A)}{2^{\lvert A\rvert}-1} e^{\sum_{B\subseteq X, B\neq A}\frac{\lvert A\cap B\rvert}{2^{\lvert X\rvert}-1}}\right)$	Entropy
Xiao [15]	$M(A) = \mathbf{m}(A)e^{i\theta(A)}$	Complex form
Pan [17]	$CM_0^j(E_p) = \left(\frac{1}{e^{\lvert\delta_p^{j'}-\delta_p^j\rvert}}\right) e^{i\left(\mu_p^{j'}-\mu_p^j\right)}$	Complex form
Xiao [23]	$BJS(m_i,m_j) = \frac{1}{2}\left[S\left(m_i,\frac{m_i+m_j}{2}\right)+S\left(m_j,\frac{m_i+m_j}{2}\right)\right]$	Divergence
Zhao [24]	$\mathrm{DHM}(m_1,m_2) = \frac{2D_{\mathrm{d}}\left(m_1\lVert\frac{2m_1m_2}{m_1+m_2}\right)D_{\mathrm{d}}\left(m_2\lVert\frac{2m_1m_2}{m_1+m_2}\right)}{D_{\mathrm{d}}\left(m_1\lVert\frac{2m_1m_2}{m_1+m_2}\right)+D_{\mathrm{d}}\left(m_2\lVert\frac{2m_1m_2}{m_1+m_2}\right)}$	Divergence
Yang [25]	$\mathrm{TU}^I(m) = 1-\frac{1}{\lvert X\rvert}\cdot\sqrt{3}\cdot\sum_{A\in X} d^I([Bel(A),Pl(A)],[0,1])$	Similarity degree
Zhang [26]	$d_{BPA}(m_i,m_j) = d_{ij} = -\ln(BC(m_i,m_j))$	Similarity degree
Xiao [27]	$d_{\mathrm{CBBA}}(\mathbb{M}_1,\mathbb{M}_2) = \sqrt{\frac{\lvert(\vec{\mathbb{M}}_1-\vec{\mathbb{M}}_2)^T\underline{\mathbb{D}}(\vec{\mathbb{M}}_1-\vec{\mathbb{M}}_2)\rvert}{\sum_{A\subseteq\Omega}\mathbb{M}_1(A)+\sum_{B\subseteq\Omega}\mathbb{M}_2(B)}}$	Similarity degree

with fuzzy theory (high trust, trust, distrust, high distrust, and uncertainty) with two elements in the FOD to express the trust degree of nodes. In this review, the application of DST in trust models is summarized in three areas.

1) Expressing trust between nodes: after selecting the appropriate trust factors, the trust between nodes is expressed through a vector composed of elements in FOD.

2) Synthesizing trust: after obtaining the direct trust, the indirect trust is represented by a trust chain consisting of multi-hop nodes. The trust of multiple nodes is combined using the D-S combination rule to obtain the synthesized indirect trust. To improve the trust degree, it is also necessary to combine the direct and indirect trusts between nodes to get the complete node trust.

3) Synthesizing all sensor nodes: all sensor nodes in the network are preprocessed to obtain the BPA of each node. The trust of sensor nodes is judged after using the D-S combination rule. The impact of malicious nodes is reduced from the fusion decision layer.

III. D-S EVIDENCE THEORY IN TRUST EVALUATION AND DECISION

Currently, distributed networks are facing a huge security threat from internal attacks. Because of the free access and movement of nodes, the topology of communication links and connections in MANET is constantly changing. Therefore, the nodes in MANET are vulnerable to be attacked. The nodes in wireless sensor network (WSN) which consists of the large number of sensor nodes are randomly deployed in network or field environments. In this case, the sensor nodes are vulnerable to be attacked and become malicious nodes. Trust model is an effective security solution to defend against internal attacks. In trust model, trust evaluation mainly includes the collection and processing of evidence and the weight assignment of evidence. Trust evaluation is a precondition for trust decision, and decisions are made based on the trust degree. In this section, DST-based trust is summarized and analyzed in terms of both trust evaluation and decision. The relationship between trust evaluation and decision is shown in Fig. 2.

A. DST-BASED TRUST EVALUATION

Feng et al. proposed a trust evaluation algorithm (NBBTE) based on node behavior policy and DST. NBBTE evaluated the trust between nodes with multivariate trust factors and got the affiliation of trust value by fuzzy theory. The integrating trust combined direct and indirect trust using the improved DST [7]. Tian et al. proposed an improved fusion scheme based on DST. This method calculated BPA of per sensor node using gray correlation to reduce the impact of

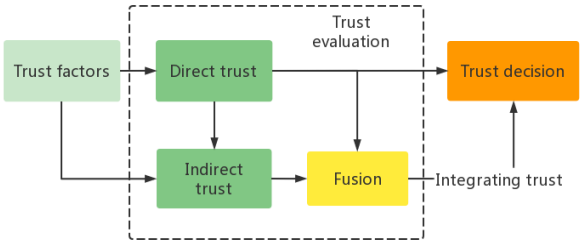


FIGURE 2. Relationship between trust evaluation and decision.

malicious nodes, while improving the anti-attack capability of WSN from the fusion decision layer and saving network overhead [8]. Sun et al. combined D-S evidence theory and ant colony algorithm to measure trust between nodes by packet reception and delivery rate, packet forwarding rate and consistency factor. The high conflict indirect trusts are assigned similarity weights and reliable routing paths are found by the ant colony algorithm, which reduced end-to-end delay and improved throughput and malicious node detection rate [28]. Yang et al. proposed a novel detection scheme based on DST in WSN. This model modified the indirect trust by defining the evidence variance. Comprehensive trust combined by direct and indirect trust using D-S combination rule can inhibit collusion of malicious nodes partly, improving security and robustness [29]. Cheng et al. proposed a hierarchical WSN trust model based on a cluster network topology. Combining the classical RFSN model, the direct trust was calculated from three aspects, such as communication trust, data transmission trust and node trust. The indirect trust was calculated from the trust matrix of the cluster head [30]. Yang et al. proposed two algorithms, NNOM-based DTV and NRTM-based ITV. Direct trust (DTV) was calculated using a watchdog mechanism to detect black hole attacks. Using D-S evidence theory combined with indirect trust (ITV) from different neighboring nodes to detect cooperative black hole attacks [31]. Wang et al. optimized the classical DST by filtering perceptual data, adjusting weights of BPA and improving the D-S combination rule. It overcame the problem of high computation and the difficulty to resolve high conflict data. So that it satisfied the requirements of real-time and reliability in autonomous driving scenarios [32]. Wu et al. proposed a data centric traffic information model (TIDTM) to evaluate trust degree of traffic information in dynamic routing. Using a voting algorithm based on DST to avoid malicious information and reduce vehicle travel time on the road. But this model is difficult to identify the malicious information when the number of malicious nodes is too high [33]. Bhargava et al. proposed DST-based edge-centric IoT trust model (DEIT). DEIT can detect both types of malicious behavior, message loss and message modification, in a very short time. DEIT also reduce the overhead of trust information in the network [34]. Liu proposed coverage reliability based on DST to judge the reliability of WSN. Meanwhile, this method reduced computational complexity [35]. Qiang et al. proposed a CS-BP neural network evaluation model based on D-S evidence theory. Combining the self-learning and adaptive nature of BP neural networks, the subjectivity of assignment was reduced in D-S evidence theory. Also, the BP neural network combining the cuckoo algorithm (CS) optimized the initial parameters to improve the training efficiency of BP neural network [36].

B. DST-BASED TRUST DECISION

Reddy et al. used packet delivery rate based on cos function to evaluate direct trust. After obtaining distance similarity between evidence, the information of neighboring nodes which are given similarity weights were combined using the D-S combination rule [37]. Zhang et al. proposed a malicious node detection scheme based on DST (NTMS-DS) for WSN. NTMS-DS considered the spatial-temporal correlation of data collected by neighbor sensor nodes and updated the direct trust of nodes by Kalman filtering. Then indirect trust calculated based on DST and the number of interactions between nodes. The integrating trust combined direct trust and indirect trust to improve malicious node detection and reduce energy loss [38]. Weeraddana et al. proposed an information processing framework for distributed WSN. Based on D-S evidence theory and evidence filtering schemes, multimodal sensor data directly processed to solve the inability to quickly and effectively communication for WSN deployed in multi-layer networks [39]. Yu et al. proposed a trust scheme based on negative binomial distribution to solve the problem of data trust in industrial wireless sensor networks (IWSN). Combining DST and noise filtering method, the reliability and robustness of the data could be improved in industrial environments [40]. Sun et al. proposed a secure routing protocol for WSN based on multi-objective ant colony optimization. Introducing Pareto optimization in ant colony algorithms and making the rest energy of the node and the trust value of the routing path as two optimization objectives to solve resource constraints and security issues in WSN. The trust model was built by improving DST [41]. Feng et al. proposed a trust management scheme based on improved DST (TMS). TMS expressed the direct trust by vector and obtaining trust value of neighbor nodes through trust evaluation and trust transfer mechanism of dynamic aggregation. To improve the trust degree of node and the robustness of the network, the trust of sensor nodes evaluated based on the BPA obtained by improved DST [42]. Rani et a. proposed a distributed trust model to detect malicious nodes based on recommendation filtering (RFTM). RFTM used beta distribution to calculate direct trust and collected information of one-hop neighbor nodes. After filtering error messages by deviation tests, RFTM combined direct and indirect trust to improve packet forwarding rate and throughout, reduced end-to-end delay and energy consumption at the same time [43]. Mahapatra et al. proposed a cluster tree enhanced DST based Bidirectional Butterfly Optimization algorithm (CT-EDS-BBO). After finding the sink node and routing path in the cluster through the routing protocol, CT-EDS-BBO evaluated node

trust degree using DST. Bidirectional Butterfly Optimization algorithm could find the best route to transmit data and reduce energy loss [44]. Kashani et al. proposed a protocol based on DST and opportunity route (DSTOR). The next reliable hop node selected by packet forwarding and vehicle density combined DST. The opportunity route protocol could reduce the number of multi-hop nodes and end-to-end delay [45]. Wang et al. proposed a distributed multi-agent resource allocation system (ITEM) to solve resource issues. The evidence theory was improved by Deng entropy and weakness factor. Using ITEM to expand the dynamic trust evaluation of multi-agent systems (MAS) and enhance selection efficiency of MAS [46].

C. COMPARISON AND ANALYSIS

Combining the overview of above schemes, this section summarizes the objective trust factors for determining whether a node is trustworthy, and trust factors in trust evaluation and trust decision are summarized as shown in table 3 and table 4. The trust factors are also extended to consider multiple subjective trust factors. The application of DST in trust is represented in detail.

1) TRUST FACTORS

Trust between nodes needs to take the consequences of being betrayed. The trust channel only appears when the current trust value exceeds the trust threshold for taking risks. In the current models, trust between nodes is usually judged quantitatively using trust factors, such as Received packet rate (RPF), Sending packet rate (SPF), Packet forwarding rate (PFR), Consistency factor (CF), Interactive time factor (ITF), Energy factor (EF), Interactive behaviors (IB), Characteristic scenarios factor (CSF).

However, node trust cannot fully and accurately express through these objective factors. An individual is influenced by his emotions when making decisions [47]. Emotions are highly connected with his past experiences, depth of thought and mood state when making decisions.Unlike an individual, a node or other intelligent device will only make a ''reason'' decision through the collected signals. Current sensor technology is developing rapidly and smart sensors are becoming able to recognize factors such as emotions [48]. Therefore, more trust factors can be added to determine whether a node is trustworthy or not, such as the trust tendency between nodes will regulate the level of trust in the nodes.

Case 1: Supposing ITF, PFR and EF are used to determine whether a node is trusted. When the interaction is fast, the packet forwarding rate is high and the energy consumption is low, it can indicate the high confidence between nodes. However, when one or both factors are lacking, not only the characteristics of the target node need to be paid attention to, the selection of the source node is also important. Based on the need of source node for information about the target node (e.g., real time requires fast node interaction characteristics), the source node will tend to choose the target node with fast interaction speed. Similarly, when the source node has limited energy, it will tend to choose the target node with low energy consumption for interaction.

2) TRUST ACQUISITION

These three cases elaborate the application of DST in trust. In case 2, it explains how DST represents direct trust, and then how to integrate trusts and integrate trusts of all sensor nodes are explained in case 3 and 4, respectively.

Case 2: Expressing trust between nodes

Suppose in a ternary trust, the RPF, SPF and PFR are used as trust factors to express the trust of a node. The direct trust is expressed as $DT_{i,j} = (m(\{T\}), m(\{-T\}), m(\{T, -T\}))$

a) $m(\{T\}), m(\{-T\})$ expressed as RPF and SPF respectively.

$$\{m(\{T\}), m(\{-T\}), m(\{T, -T\})\} = \{RPF, SPF, 1-RPF-SPF\}. \quad (8)$$

b) The elements in the power set expressed by the trust factors assigned weights.

$$\begin{aligned} &DT_{i,j} \\ &= (m(\{T\}), m(\{-T\}), m(\{T, -T\})) \\ &= \begin{cases} m(\{T\}) = \omega_1 \cdot RPF^1_{i,j} + \omega_2 \cdot SPF^1_{i,j} + \omega_3 \cdot PFR^1_{i,j} \\ m(\{-T\}) = \omega_1 \cdot RPF^0_{i,j} + \omega_2 \cdot SPF^0_{i,j} + \omega_3 \cdot PFR^0_{i,j} \\ m(\{T, -T\}) = 1 - m(\{T\}) - m(\{-T\}) \end{cases} \end{aligned} \quad (9)$$

w_1, w_2, w_3 are artificially set weights, and $w_1 + w_2 + w_3 = 1$.

Case 3: Synthesizing trust

Supposing S1 is the source node, S2 is the target node, and C1, C2, C3, C4 are the third-party nodes, as shown in Fig. 3.

a) Because the nodes trust varies from C1 to C4, it is difficult to make a correct judgment on the single node. The source node needs to obtain the trust of the third-party node from the target node. The integrating trust of target node is obtained from the combined third-party nodes.

b) The trust also exists between the target node and the source node and this trust is more intuitive. The direct trust is crucial in determining whether the node is trusted. Therefore, the indirect trust and direct trust between nodes need to be integrated.

Case 4: Synthesizing all sensor nodes

Supposing all the sensor nodes from S1 to Sn are need to be judged in the network as shown in Fig. 4. BPA is obtained by preprocessing all sensor nodes and combined by D-S combination rule. The information is calculated and analyzed from the fusion decision level to improve the accuracy of decision making.

3) THE REASONS FOR DST IN TRUST MODEL

D-S evidence theory as a generalization of bayesian theory [49] maintains the observation of the data but expresses uncertainty well without the requirement of knowing prior probabilities. In trust evaluation, for different scenarios of

TABLE 3. Comparison of different schemes.

Schemes	Trust factors								Performances
	RPF	SPF	PFR	CF	ITF	EF	IT	CSF	
NBBTE [7]	✓	✓	✓	✓	✓				Higher MDP, Higher AEC
Sun [28]	✓	✓	✓	✓					Higher MDP, Lower TD
Yang [29]	✓	✓					✓		High MDP, Higher AEC
Yang [31]	✓	✓							High MDP
DEIT [34]	✓	✓	✓		✓		✓		Higher MDP, Lower TL
TWSN [37]	✓	✓	✓						Lower AEC, High PFR
NTMS-DS [38]				✓	✓		✓		Higher MDP, Higher AEC
SRPMA [41]	✓	✓		✓					Higher AEC, Lower PFR
TMS [42]	✓	✓	✓						Higher MDP, Medium AEC
RFTM [43]	✓	✓	✓						Lower TDLower AEC, Higher PRF
CT-EDS-BBOA [44]				✓	✓	✓		✓	Higher PFR, Lower AEC
DSTOR [45]	✓	✓	✓					✓	Low TD, High PFR
ITEM [46]	✓	✓					✓	✓	Lower TD, Higher PFR
Tian [8]	Evaluate all sensor node trust								Low TD, High MDP
Wang [32]	Evaluate all sensor node trust								Low TD, High Robustness

Vertical Note: The meaning of each abbreviation in performance. Malicious nodes detection rate (MDP), Time latency (TL), Average energy consumption (AEC), Packet Forwarding Ratio (PFR).

TABLE 4. DST in different schemes.

Schemes	Expressing trust between nodes	Synthesizing trust		Synthesizing all sensor nodes	Improvements
		Direct	Indirect		
NBBTE [7]	✓		✓		Similarity degree
Tian [8]	✓			✓	Modifying combination rule
Sun [28]	✓		✓		Similarity degree
Yang [29]	✓		✓		Similarity degree
Yang [31]			✓		Similarity degree
Wang [32]	✓			✓	Similarity degree , Modifying combination rule
DEIT [34]	✓	✓	✓		None
TWSN [37]			✓		Similarity degree
NTMS-DS [38]	✓		✓		Similarity degree
SRPMA [41]	✓	✓	✓		Similarity degree
TMS [42]	✓		✓		Similarity degree
RFTM [43]			✓		None
CT-EDS-BBOA [44]	✓			✓	Similarity degree
DSTOR [45]	✓	✓	✓		None
ITEM [46]	✓	✓	✓		Entropy, Modifying combination rule

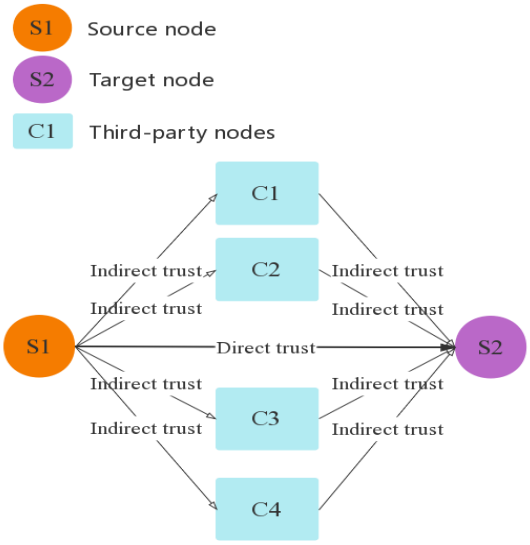


FIGURE 3. Diagram of direct and indirect trust.

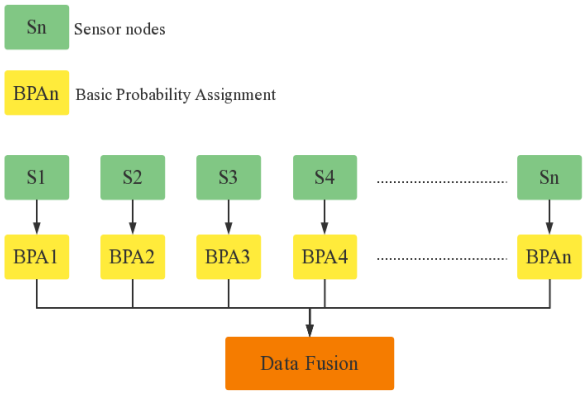


FIGURE 4. Synthesizing all sensor nodes' trust.

trust factors (road information in vehicle networks, communication interference in underwater wireless sensor networks, etc.), multiple trust factors can be combined by framework of discernment to express the uncertainty of trust degree between nodes.

DST is different from other approaches to deal with uncertainty such as fuzzy logic, game theory and cloud model. The fuzzy logic uses the membership grade and the membership function to obtain the node trust values by defuzzification [50]. Game theory makes decisions by judging the

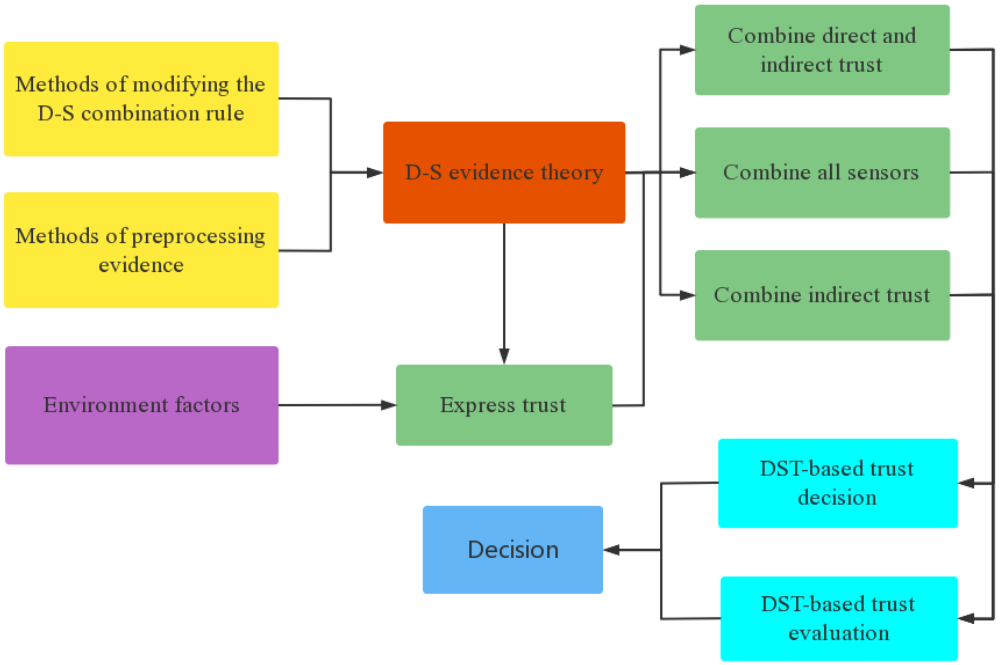


FIGURE 5. Structure of DST-enabled trust.

benefits that can be gained from this cooperation [51]. The cloud model achieve qualitative and quantitative transformation of node trust degree by expectation, entropy and hyperentropy [52]. They all have a common characteristic of being unable to handle multiple trust. However, DST can synthesize the trust of multiple nodes on the target node. When using DST for trust decision, more available information can be judged and the judgment of the target node can be strengthened. The structure of DST-enabled trust is shown in Fig. 5.

IV. FUTURE RESEARCH DIRECTIONS

Although many DST-based models have been proposed to defend against the attacks and improve the identification of malicious nodes. There are still some future research directions need to be concerned.

A. DST-BASED MALICIOUS NODES AUTO-EXCLUSION MECHANISM IN TRUST MANAGEMENT

Many trust models have used DST to solve problems in trust models to improve malicious node detection rates. The existing method can identify malicious nodes quickly and accurately, but it is difficult to locate the malicious node, and it is unable to determine whether the malicious node is masquerading as a normal node. In the future, it can be combined with node location algorithms to locate the malicious nodes precisely and make sure malicious nodes are removed from network routing as well as location lists to avoid the potential danger of data theft. Submitting the authenticity of location services and reducing the possibility of neighboring nodes being complicit in malicious nodes to reduce network overhead.

B. LOW COMPLEXITY COMPUTATIONAL SCHEME FOR D-S COMBINATION RULE

With the development of network, the number of deployed sensor nodes [8], [32] and the need for routing paths [41] become larger. The demand for computational skills also increases. As the number of elements in the recognition framework increases [34], the calculation volume when using combination rule increases exponentially. Limited by the lack of sensor node computing, storage, and energy supply capacity [53], it is difficult to run algorithms with high computational complexity for a long time. The overly complex calculations are difficult to meet the needs of some real-time services. In the future, mathematical schemes such as matrix analysis and convex optimization can be combined to further reduce the computational complexity of combination rules. The low complexity computational can also improve computational efficiency to reduce sensor node energy loss and extend network operation time.

C. EMOTION-BASED TRUST FACTOR EXPRESSION SCHEME IN TRUST MODEL

It is important for network to judge the trust degree of nodes. Different trust factors are used in different trust models [28], [29], [30], [38], [41], [42], and the use of multiple trust factors is more trustworthy than single trust factors. At present, factors such as emotion are gradually being recognized by sensors. Emotion-based trust factors can describe the current state of the node more perfectly and solve the shortage of objective factors. In the future, the emotion-based trust factors of nodes such as tendency and willingness can be considered to selectively interact with nodes. In this way,

the energy loss of nodes will be reduced and the network utilization will be improved.

V. CONCLUSION

The technical characteristics and application scenarios of distributed network nodes make the node trust particularly important. Considering that DST can well solve the uncertainty of trust management process, the main contributions of this review are: 1. The DST-based trust is analyzed and summarized from trust evaluation and trust decision. Large number of models and analyses show that the DST can well handle the uncertainty of trust factors of nodes in distributed networks and improve the identification rate of malicious nodes. 2. Future research directions are given, which include three areas: auto-exclusion of malicious nodes, low computational complexity of D-S combination rules, and emotion-based trust factors. In summary, this review will help improve the trust of sensor nodes and improve the reliability of the network.

REFERENCES

[1] N. Djedjig, D. Tandjaoui, I. Romdhani, and F. Medjek, "Trust management in the Internet of Things," in *Security and Privacy in Smart Sensor Networks*. Hershey, PA, USA: IGI Global, 2018, pp. 122–146, doi: 10.4018/978-1-5225-5736-4.ch007.

[2] V. Adat and B. B. Gupta, "Security in Internet of Things: Issues, challenges, taxonomy, and architecture," *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, 2018, doi: 10.1007/s11235-017-0345-9.

[3] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, "Trust-based attack and defense in wireless sensor networks: A survey," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–20, Sep. 2020, doi: 10.1155/2020/2643546.

[4] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019, doi: 10.1109/ACCESS.2018.2880838.

[5] W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A trust-based security system for data collection in smart city," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4131–4140, Jun. 2021, doi: 10.1109/TII.2020.3006137.

[6] W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks," *Digit. Commun. Netw.*, vol. 7, no. 4, pp. 470–478, Nov. 2021, doi: 10.1016/j.dcan.2021.03.005.

[7] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, Feb. 2011. [Online]. Available: https://www.mdpi.com/1424-8220/11/2/1345

[8] Q. Tian, P. Qin, M. Wang, and Y. Liu, "D-S based fusion method for against malicious nodes in wireless sensor networks," Presented at the IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Jul. 2020.

[9] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *Ann. Math. Statist.*, vol. 38, no. 2, pp. 325–339, Apr. 1967, doi: 10.1214/aoms/1177698950.

[10] K. Zhao, L. Li, Z. Chen, R. Sun, G. Yuan, and J. Li, "A survey: Optimization and applications of evidence fusion algorithm based on Dempster–Shafer theory," *Appl. Soft Comput.*, vol. 124, Jul. 2022, Art. no. 109075, doi: 10.1016/j.asoc.2022.109075.

[11] W. Ma, Y. Jiang, and X. Luo, "A flexible rule for evidential combination in Dempster–Shafer theory of evidence," *Appl. Soft Comput.*, vol. 85, Dec. 2019, Art. no. 105512, doi: 10.1016/j.asoc.2019.105512.

[12] R. R. Yager, "On the Dempster–Shafer framework and new combination rules," *Inf. Sci.*, vol. 41, no. 2, pp. 93–137, Mar. 1987, doi: 10.1016/0020-0255(87)90007-7.

[13] D. Dubois and H. Prade, "Representation and combination of uncertainty with belief functions and possibility measures," *Comput. Intell.*, vol. 4, no. 3, pp. 244–264, Sep. 1988, doi: 10.1111/j.1467-8640.1988.tb00279.x.

[14] C. K. Murphy, "Combining belief functions when evidence conflicts," *Decis. Support Syst.*, vol. 29, no. 1, pp. 1–9, Jul. 2000, doi: 10.1016/S0167-9236(99)00084-6.

[15] F. Xiao, "Generalization of Dempster–Shafer theory: A complex mass function," *Int. J. Speech Technol.*, vol. 50, no. 10, pp. 3266–3275, Oct. 2020, doi: 10.1007/s10489-019-01617-y.

[16] F. Xiao and W. Zhang, "Generalized belief function in complex evidence theory," *J. Intell. Fuzzy Syst.*, vol. 38, no. 4, pp. 3665–3673, Apr. 2020, doi: 10.3233/jifs-179589.

[17] L. Pan and Y. Deng, "A new complex evidence theory," *Inf. Sci.*, vol. 608, pp. 251–261, Aug. 2022, doi: 10.1016/j.ins.2022.06.063.

[18] Y. Deng, "Uncertainty measure in evidence theory," *Sci. China Inf. Sci.*, vol. 63, no. 11, Nov. 2020, Art. no. 210201, doi: 10.1007/s11432-020-3006-9.

[19] R. R. Yager, "Entropy and specificity in a mathematical theory of evidence," *Int. J. Gen. Syst.*, vol. 9, no. 4, pp. 249–260, 1983, doi: 10.1080/03081078308960825.

[20] D. Dubois and H. Prade, "Properties of measures of information in evidence and possibility theories," *Fuzzy Sets Syst.*, vol. 100, pp. 35–49, Jan. 1999, doi: 10.1016/S0165-0114(99)80005-0.

[21] Y. Deng, "Deng entropy," *Chaos, Solitons Fractals*, vol. 91, pp. 549–553, Oct. 2016, doi: 10.1016/j.chaos.2016.07.014.

[22] H. Cui, Q. Liu, J. Zhang, and B. Kang, "An improved Deng entropy and its application in pattern recognition," *IEEE Access*, vol. 7, pp. 18284–18292, 2019, doi: 10.1109/ACCESS.2019.2896286.

[23] F. Xiao, "Multi-sensor data fusion based on the belief divergence measure of evidences and the belief entropy," *Inf. Fusion*, vol. 46, pp. 23–32, Mar. 2019, doi: 10.1016/j.inffus.2018.04.003.

[24] K. Zhao, R. Sun, L. Li, M. Hou, G. Yuan, and R. Sun, "An optimal evidential data fusion algorithm based on the new divergence measure of basic probability assignment," *Soft Comput.*, vol. 25, no. 17, pp. 11449–11457, Sep. 2021, doi: 10.1007/s00500-021-06040-5.

[25] Y. Yang and D. Han, "A new distance-based total uncertainty measure in the theory of belief functions," *Knowl.-Based Syst.*, vol. 94, pp. 114–123, Feb. 2016, doi: 10.1016/j.knosys.2015.11.014.

[26] W. Zhang, X. Ji, Y. Yang, J. Chen, Z. Gao, and X. Qiu, "Data fusion method based on improved D-S evidence theory," Presented at the IEEE Int. Conf. Big Data Smart Comput. (BigComp), Jan. 2018.

[27] F. Xiao, "CED: A distance for complex mass functions," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 4, pp. 1525–1535, Apr. 2020, doi: 10.1109/TNNLS.2020.2984918.

[28] Z. Sun, Z. Zhang, C. Xiao, and G. Qu, "D-S evidence theory based trust ant colony routing in WSN," *China Commun.*, vol. 15, no. 3, pp. 27–41, Mar. 2018, doi: 10.1109/CC.2018.8331989.

[29] K. Yang, S. Liu, X. Li, and X. A. Wang, "D-S evidence theory based trust detection scheme in wireless sensor networks," *Int. J. Technol. Hum. Interact.*, vol. 12, no. 2, pp. 48–59, Apr. 2016, doi: 10.4018/ijthi.2016040104.

[30] X. Cheng, Y. Luo, and Q. Gui, "Research on trust management model of wireless sensor networks," in *Proc. IEEE 3rd Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Oct. 2018, pp. 1397–1400, doi: 10.1109/IAEAC.2018.8577648.

[31] B. Yang, R. Yamamoto, and Y. Tanaka, "Dempster-shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs," Presented at the 16th Int. Conf. Adv. Commun. Technol. (ICACT), Pyeongchang, South Korea, Feb. 2014.

[32] P. Wang, X. Wen, L. Wang, Z. Lu, and L. Ma, "An improved D-S based vehicular multi-Sensors' perceptual data fusion for automated driving decision-making," Presented at the IEEE 90th Veh. Technol. Conf. (VTC-Fall), Sep. 2019.

[33] Y. Wu, F. Meng, G. Wang, and P. Yi, "A Dempster–Shafer theory based traffic information trust model in vehicular ad hoc networks," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Shanghai, China, Aug. 2015, pp. 1–7, doi: 10.1109/SSIC.2015.7245329.

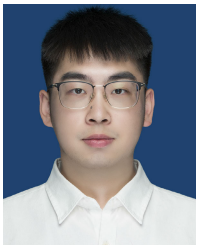
[34] A. Bhargava and S. Verma, "DEIT: Dempster Shafer theory-based edge-centric Internet of Things-specific trust model," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, Jun. 2021, Art. no. e4248, doi: 10.1002/ett.4248.

[35] Q. Liu, "Coverage reliability evaluation of wireless sensor network considering common cause failures based on D–S evidence theory," *IEEE Trans. Rel.*, vol. 70, no. 1, pp. 331–345, Mar. 2021, doi: 10.1109/TR.2020.2999576.

[36] J. Qiang, F. Wang, and X.-L. Dang, "Network security based on D-S evidence theory optimizing CS-BP neural network situation assessment," Presented at the 5th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/4th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom), Jun. 2018.

[37] V. Busi Reddy, S. Venkataraman, and A. Negi, "Communication and data trust for wireless sensor networks using D–S theory," *IEEE Sensors J.*, vol. 17, no. 12, pp. 3921–3929, Jun. 2017, doi: 10.1109/JSEN.2017.2699561.
[38] W. Zhang, S. Zhu, J. Tang, and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *J. Supercomput.*, vol. 74, no. 4, pp. 1779–1801, Apr. 2018, doi: 10.1007/s11227-017-2150-3.
[39] D. M. Weeraddana, C. Kulasekere, and K. S. Walgama, "Dempster–Shafer information filtering framework: Temporal and spatio-temporal evidence filtering," *IEEE Sensors J.*, vol. 15, no. 10, pp. 5576–5583, Oct. 2015, doi: 10.1109/JSEN.2015.2442153.
[40] S. Yu and J. He, "Providing trusted data for industrial wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, pp. 1–7, Dec. 2018, doi: 10.1186/s13638-018-1307-y.
[41] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks," *Appl. Soft Comput.*, vol. 77, pp. 366–375, Apr. 2019, doi: 10.1016/j.asoc.2019.01.034.
[42] R. Feng, S. Che, X. Wang, and N. Yu, "Trust management scheme based on D-S evidence theory for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 6, Jun. 2013, Art. no. 948641, doi: 10.1155/2013/948641.
[43] R. John and J. Deepa, "Trust model for secure routing in wireless sensor network using AI technique," Presented at the 8th Int. Conf. Smart Struct. Syst. (ICSSS), Apr. 2022.
[44] S. N. Mahapatra, B. K. Singh, and V. Kumar, "Secure energy aware routing protocol for trust management using enhanced dempster Shafer evidence model in multi-hop UWAN," *Wireless Netw.*, vol. 28, no. 7, pp. 3059–3076, Oct. 2022, doi: 10.1007/s11276-022-03021-w.
[45] A. A. Kashani, M. Ghanbari, and A. M. Rahmani, "Improving the performance of opportunistic routing protocol using the evidence theory for VANETs in highways," *IET Commun.*, vol. 13, no. 20, pp. 3360–3368, Dec. 2019, doi: 10.1049/iet-com.2019.0473.
[46] N. Wang, H. Zgaya-Biau, P. Mathieu, and S. Hammadi, "An improved evidence theory-based trust model for multiagent resource allocation," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2020, pp. 600–607, doi: 10.1109/SMC42975.2020.9283483.
[47] D. Carnagey, "Influencing by suggestion" in *The Art of Public Speaking*. Urbana, IL, USA: Project Gutenberg, 2005, pp. 262–280. [Online]. Available: https://www.gutenberg.org/ebooks/16317
[48] P. Leelaarporn, P. Wachiraphan, T. Kaewlee, T. Udsa, R. Chaisaen, T. Choksatchawathi, R. Laosirirat, P. Lakhan, P. Natnithikarat, K. Thanontip, W. Chen, S. C. Mukhopadhyay, and T. Wilaiprasitporn, "Sensor-driven achieving of smart living: A review," *IEEE Sensors J.*, vol. 21, no. 9, pp. 10369–10391, May 2021, doi: 10.1109/JSEN.2021.3059304.
[49] A. P. Dempster, "A generalization of Bayesian inference," *J. Roy. Stat. Soc. B, Methodol.*, vol. 30, no. 2, pp. 205–232, 1968, doi: 10.1111/j.2517-6161.1968.tb00722.x.
[50] L. Yang, Y. Lu, S. X. Yang, T. Guo, and Z. Liang, "A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4837–4847, Jul. 2021, doi: 10.1109/TII.2020.3019286.
[51] V. Sankaranarayanan, M. Chandrasekaran, and S. Upadhyaya, "Towards modeling trust based decisions: A game theoretic approach," presented at the ESORICS, in Lecture Notes in Computer Science, vol. 4734, J. Biskup and J. López, Eds. Heidelberg, Germany: Springer, 2007, pp. 485–500, doi: 10.1007/978-3-540-74835-9_32.
[52] L. Yang, K. Yu, S. X. Yang, C. Chakraborty, Y. Lu, and T. Guo, "An intelligent trust cloud management method for secure clustering in 5G enabled Internet of Medical Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 8864–8875, Dec. 2022, doi: 10.1109/TII.2021.3128954.
[53] W. Fang, C. Zhu, F. R. Yu, K. Wang, and W. Zhang, "Towards energy-efficient and secure data transmission in AI-enabled software defined industrial networks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 4265–4274, Jun. 2022, doi: 10.1109/TII.2021.3122370.

WUXIONG ZHANG (Member, IEEE) received the B.E. degree in information security from Shanghai Jiao Tong University, Shanghai, China, in 2008, and the Ph.D. degree in communication and information systems from the Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai, in 2013. He is currently a Professor with SIMIT. His research interests include beyond third-generation mobile communication systems and vehicular networks.



HAOHUI SUN received the B.E. degree from the North China University of Water Resources and Electric Power. He is currently pursuing the M.E. degree with the Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai, China. His research interests include trust model and information security in distributed networks.

WEIDONG FANG (Member, IEEE) received the B.E. degree in industrial electrical automation from Shandong University, Jinan, China, in 1993, the M.E. degree in communication and electronic systems from the China University of Mining and Technology, Beijing, in 1998, and the Ph.D. degree in electromagnetic fields and microwave techniques from Shanghai University, Shanghai, China, in 2016. He is currently an Associate Professor with the Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai. His research interests include information security and energy efficiency in the IoT/WSN/VANET, including trust model, secure network coding, and secure routing protocol.

CHUNSHENG ZHU (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from The University of British Columbia, Canada, in 2016. He is currently an Associate Professor with the College of Big Data and Internet, Shenzhen Technology University, China. He has authored more than 100 publications. His research interests include the Internet of Things, wireless sensor networks, cloud computing, big data, social networks, and security.

GUOQING JIA received the B.E. degree in information engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2007, and the Ph.D. degree in communication and information systems from the Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai, China, in 2013. He is currently a Professor with Qinghai Minzu University. His research interest includes mobile communication algorithm and systems.