Wireless Networks
https://doi.org/10.1007/s11276-019-02129-w

TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing

Weidong Fang[1,2] · Wuxiong Zhang[1,2] · Wei Chen[3] · Yang Liu[1,2] · Chaogang Tang[3]

Abstract
Based on fog computer, an industrial wireless sensor network (F-IWSN) is a novel wireless sensor network in the industry. It not only can more efficiently reduce information transmission latency, but also can more beneficially achieve the real-time control and the rapid resource scheduling. However, similar to other distributed networks, it also faces enormous security challenges, especially those internal attacks. The differences from those traditional security schemes are that, one is the trade-off between security, transmission performance and energy consumption to meet the requirements of information convergence and control, the other constructs a multi-dimensional selective forwarding scheme to achieve the real time transmission. In this paper, we propose a Gaussian distribution-based comprehensive trust management system (GDTMS) for F-IWSN. Furthermore, in its trust decision, the grey decision making is introduced to achieve the trade-off between security, transmission performance and energy consumption. The proposed trade-off can effectively select the secure and robust relay node, namely, a trust management-based secure routing scheme. In addition, the proposed schemes are also applicable to defending against bad mouthing attacks. Simulation results show that, the comprehensive performance of GDTMS is better than other similar algorithms. It can effectively prevent the appearance of network holes, and balance the network load, promote the survivability of the network.

Keywords 5G · Industrial wireless sensor network (IWSN) · Fog computing · Secure routing protocol · Trust management

1 Introduction

As the next-generation broadband wireless communication network, the main goal of 5G networks is to keep end users connected. The devices that 5G networks will support in the future are much more than just smart phones—it also supports a variety of smart terminals. In the past few years, with the 5G network development, the industrial wireless sensor network (IWSN) has been successfully deployed in industrial fields, such for safety protection, production supervision, data acquisition, and control etc. In IWSN, the sensed information can communicate from the nodes to the supervisory control and data acquisition systems for processing and controlling purposes. Based on these observations, the central manager can control the producing processes, or directly command a mobile worker at the plant. Hence, the risk of equipment damage is reduced, and efficiency and productivity are increased. IWSN bring several advantages over conventional wired industrial networks in terms of infrastructure (no long cable runs), ease of troubleshooting, and rapid deployment [1, 2]. Furthermore, combined with cloud computing, IWSNs can offer more economical solutions in many harsh environments where it is difficult to deploy wires.

The cloud computing has inherent advantages: elasticity and scalability, and three key facts, including Isis (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service). It has provided many opportunities

✉ Wei Chen
chenw@cumt.edu.cn

[1] Key Laboratory of Wireless Sensor Network and Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200051, China

[2] Shanghai Research Center for Wireless Communication, Shanghai 201210, China

[3] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, Jiangsu, China

Published online: 07 September 2019

and conveniences for the manufacturing industry. However, it is limited by the distance between the terminal devices and the cloud, which will cause significant latency, and bring many issues for latency-sensitive applications (i.e. real-time control, monitoring parameters). Currently, the cloud computing paradigm can hardly meet the requirements regarding to the mobility support, the location awareness and the low latency. In addition, it alone does not support 5G and AI (Artificial Intelligence). Benefiting from distributed computing, the emerging fog computing [3] can tackle the above issues. Fog is "cloud closer to ground". It is a novel paradigm extending traditional cloud computing to service to the edge of the network. Similar to Cloud, Fog provides computational, networking and storage services to terminal-users. In a sense, the fog computing is also a paradigm of 5G flat management. However, different from Cloud, Fog provides additional advantages such as distributed characters.

Due to its distributed feature, the fog computing can provide the services outside the cloud, at the edge of the network and closer to terminal devices. It has several technical innovations with the following aspects: storage, communication, as well as control, configuration, measurement and management. Hence, it can provide low latency, location awareness, and improved Quality of Services (QoS) for those streaming and real time applications. It also supports densely distributed data collection. The fog computing is well positioned for many application scenarios, which involve the vehicle to everything (V2X) [3], smart grid [4], as well as software-defined networking (SDN) [5]. In a word, the fog computing is introduced into IWSN, namely fog-assisted industrial wireless sensor network (F-IWSN).

Practically, just as classical IWSN, the F-IWSN is more preferred in harsh industrial environments, which involve high temperatures, high humidity, stronger noise, and so on. These extreme conditions can cause unpredictable interference on wireless channels. Moreover, the monitoring and controlling process with maximum accuracy is required in industry, which also reduces the risk of equipment damage. Some critical industrial applications need the real-time communication, that is, a task must be done within a specific time interval. These features demand the reliability, latency, and real-time communication of F-IWSN.

Furthermore, compared with the wireless sensor network (WSN), F-IWSN not only has stronger security requirements, but also faces more security challenges. F-IWSN needs to detect the malicious nodes quickly, and defend against them effectively, when the network is invaded or attacked. Nonetheless, the harsh deployed environments lead to the obvious degradation of the wireless channel quality, which increases the packet loss rate. In such a context, it is very difficult to distinguish between the normal noise and the jamming attacks [6], especially, those internal attacks (i.e. black hole attack, selective forwarding attack, and tampering attack). In addition, once these unauthorized nodes access into F-IWSN, it will lead to information disclosure. Even worse, it will impact on the monitoring and controlling of the production line, and result in the safety accidents.

From the above analysis, most of security threats in F-IWSN come from the internal attacks. The traditional cyber security schemes, including encryption and authentication, cannot defend against the internal attacks. Research has shown that the trust management scheme is an effective technology to defend against the internal attack. Hereby, a novel trust management scheme based on the Gaussian distribution is proposed to defend against On–Off attack, a typical internal attack, and to meet the low latency requirement for F-IWSN simultaneously. The rest of this paper is organized as follows: in Sect. 2, the security threats and their countermeasures in IWSN are discussed, and the detection and defense schemes against On–Off attack are reviewed. The Gaussian Distribution-based Trust Management Scheme (GDTMS) for F-IWSN is proposed, especially trust management-based secure routing scheme (TMSRS) in Sect. 3. Furthermore, the proposed scheme is simulated and analyzed in Sect. 4. Finally, the conclusion is given in Sect. 5.

2 Related works

In this section, we will investigate the security threats and their countermeasures in IWSN in terms of internal attacks and external attacks. Moreover, we will review and analyze the trust management.

2.1 Security threats and countermeasures in IWSN

1. Security threats

For IWSN, the security threats come from the security attacks, which are classified as external attacks and internal attacks.

(a) External attacks

Under external attacks, the malicious nodes are usually unauthorized or Illegal. The external attacks consist of passive attacks and active attacks. For passive attacks, the attacker can 'listen' and analyze data packets without interference, including eavesdropping and traffic analysis. In contrast, the active attacks that the attacker launch

disrupts network functionality by introducing just as jamming attacks and power exhaustion attacks.

1. Passive attacks

Eavesdropping attack: an attacker wiretaps network to obtain information in illegal ways [7]. This is due to that the broadcast characteristic and openness of the wireless medium, IWSN is vulnerable to be eavesdropped [6].

Traffic analysis: an attacker can obtain the source and destination node addresses, as well as their route by monitoring and analyzing PDUs (Protocol Data Units), and further conclude the network topology and routing algorithm to launch the tamper attack. Also, because of the openness of wireless channels, the attacker does not need a physical link to analyze traffic actually.

2. Active attacks

Jamming attack: an attacker intentionally transmits wireless signals for disrupting the data communications between the source nodes and destination nodes in IWSN. Since 2.4 GHz is usually facilitated in IWSN, the attacker can launch this attack to interference the network by using Wi-Fi or Bluetooth devices which are under the same frequency spectrum.

Power exhaustion attack [8]: the lifetime of the network depends on the battery power of the node, so an attack can make the node to consume its battery power with transmitting unnecessary signals rapidly. This attack is unique for resource-constrained nodes as it is performed by utilizing vulnerabilities of wireless networks.

(b) Internal attacks

The internal attacks are mainly launched by the compromised nodes. Compared with disabled nodes, compromised nodes actively seek to paralyze the network. They can achieve to modify the traffic flow and disrupt services by selective forwarding, tampering, or replaying.

Modifying traffic flow: the selective forwarding attack refers to the malicious node selectively to discard some received packets or completely discard the received packets without forwarding. The tamper attack can maliciously modify the transmitting data packet via the network. In wormhole attack, an attacker establishes a hypothetical tunnel with two ends through the wireless link. Multi-hop routing nodes think that there is a single hop between them. Thereby, the malicious node attracts nearby nodes to transmit data packets via this wrong path, and achieve to destroy the network. An attacker that launched Sybil attack masquerades as nodes which have multiple identities, to destroy the reputation system of peer-to-peer (P2P) network.

Disrupting service: the DoS attack (Denial of Service) can cause IWSN not to provide services properly. There are two types DoS attacks in IWSN. The former is a malicious node acting as the proxy node to deny the access-request of normal nodes. The latter is an attacker tampering the DLPDU (Data Link Protocol Data Unit), recalculating the CRC (Cyclic Redundancy Check), and transmits these packets continuously. The receiver always checks the integrity of packets, which are transmitted by malicious nodes. By checking the wrong MIC (Message Integrity Code), the receiver discards the wrong packets and requests for the packet retransmission.

3. Countermeasures

In this part, we review the security services that are provided by IEEE STD 802.15.4, and then discuss the corresponding countermeasures for each attack mentioned above.

(a) Basic security service by IEEE STD 802.15.4

IEEE STD 802.15.4, provides two security services: point-to-point security and end to-end security.

1. Point-to-point transmission security

In the data-link layer, the data encryption and MIC are deployed to guarantee the point-to-point data security using AES-CCM (Advanced Encryption Standard-Continuous Conduction Mode) mode (Counter with CBC-MAC). This mode involves two parts: in Cipher Block Chaining-Message Authentication Code (CBC-MAC) mode, the string that includes key, DLPDU header, DLPDU payload and nonce is divided into several 16-bytes sub-strings. One of the 16-bytes sub-strings are set to calculate the MIC by using the key and AES in order to provide the integrity check, meanwhile, the nonce is introduced to defend against the replay attack. In counter mode, the 16-bytes sub-string in CBC-MAC mode and the encrypted counter are taken as the input to calculate the cipher text to achieve the confidentiality of the information. The point-to-point transmissions security can detect the unidentified devices, which try to access the network without authentication, and defend against eavesdropping attacks for transmitting data in wireless medium.

2. End-to-end transmission security

In the application layer (AL), the data encryption and MIC are used to ensure the communication security between the source node and the destination node. Similarly, the AES-CCM mode as above mentioned can be deployed. MIC is calculated over AL key and AL payload to implement the integrity check.

(b) Countermeasures

Eavesdropping: two above mentioned security services can defend against the eavesdropping attacks. Regularly

updating key can make that it is difficult for an attacker to obtain it. In addition, a key can be also generated based on stochastic physical characteristics of the wireless propagation [6]. The other idea is that make the signal difficult to be captured for an attacker. For example, the frequency-hopping scheme is used in WIA-PA [7]. Besides, the specifically-designed noise may be generated to interfere with the eavesdropper without impacting on the receiving of the sink node. In addition, the beam-forming technology may be exploited to transmit the signal in a specific direction, so that the sink node receives the constructive interference signal, whereas the eavesdropper receives the destructive interference signal. However, both of them consume additional energy for generating the artificial noise, or exhibit a high computational complexity with the beam-forming design. Therefore, the diversity technology can be used to solve these issues. Currently, the diversity technology is commonly used to improve the security. They include multi-user diversity, multi-antenna diversity, and cooperative diversity [9]. Sun et al. [10] applied fountain coding to achieve secure cooperative transmission in IWSN.

Traffic analysis: point-to-point security mechanism can defend against traffic analysis effectively. However, the intermediate routing node must decrypt the data packets to obtain the destination address and the routing information, and transmits them to the destination node after they have been encrypted. It can bring additional time overhead.

Jamming and power exhaustion attack: the jamming or interference signal will result in abnormal changes of the received signal strength (RSS) and packet error rate (PER) in IWSN [11], then further these two measurements could be used to detect the jamming power exhaustion attack. Frequency hopping is an effective anti-interference paradigm. The carrier frequency of wireless signal can be changed by a known pseudo-random sequence in the sink node. In addition, the direct sequence spread spectrum (DSSS) technology can spread a transmit signal over an extremely wide frequency bandwidth. In this way, the transmit signal will have a very low power spectral density. It is difficult to demodulate the DSSS modulated signal from the background interference for the jamming attackers, so that they cannot track and interfere with the information transmission between sensor nodes and sink nodes. Chiwewe et al. [12] proposed and integrated cognitive radio technique into IWSNs to enhance the detection and defense ability for the interference. Zhang et al. [13] considered the resulting optimization problem is nonconvex for the scenario with cooperative jamming, and then proposed a heuristic algorithm based on alternating optimization.

Selective forwarding and tempering: malicious nodes can be removed by authorization and authentication. The security administrator has been set up to implement this work in the above three standards [14]. The network administrator is responsible for regularly collecting device status to evaluate and diagnose the network performance. This approach can detect and mitigate this attack to some extent. In addition, the check for MIC could guarantee the data integrity, and effectively defend against data tampering. In case of no access to key information, it is very difficult to launch a tampering attack for an attacker. Besides, the authorization and authentication for all nodes can defend against wormhole attacks and Sybil attacks.

DoS attack: authentication for nodes can defend against DoS attack in some extent. Lee et al. [15] proposed Flex-iCast, which presents an energy-efficient method to check the integrity of software objects being installed by reprogrammable sensor nodes in industrial wireless active sensor networks.

From the above analysis, the security guarantee in IWSN mainly comes from encryption, authorization, authentication, signal processing, as well as some management regulations. Admittedly, these approaches can improve the content security of IWSN. However, they are suitable for defending against external attacks, and seem powerless for internal attacks. This is due to the fact that the internal attacks are launched by compromised nodes [16], which can steal secrets from the encrypted data passed them, report other normal nodes as compromised nodes, and breach routing by introducing many routing attacks. Meanwhile, the encryption, authorization and authentication are deployed to require more computing and storage resources, this is an enormous challenge for the resource-constrained IWSN.

More and more researches show that the trust management technology is a better approach to defend against the internal attacks. In next sub-section, we will discuss a typical internal attack—On–Off attack, and analyze various defense schemes (including trust management) against it.

2.2 Trust management

Currently, one of the effective ways to defend against internal attack is trust management technologies, which are involved trust model, trust management scheme, and protocol optimization.

1. Trust model

Ganeriwal et al. [17] proposed the reputation-based framework for high integrity sensor networks (RFSN). Then, based on Beta distribution and Bayesian formula, the Beta reputation system for sensor networks (BRSN) was proposed. The BRSN was a simple trust evaluation system and it had been widely studied and used. Firoozi et al. [18] still followed the classical trust model Beta reputation, use

time windows to subdivide time slot in a hierarchical network, and the trust values of different clusters were averaged and normalized. Sinha [19] proposed the Gaussian trust and reputation for fading MIMO (Multi-Input Multi-Output) WSNs. Based on multivariate Gaussian distribution and Bayesian theorem, they considered the impact of the MIMO wireless fading channel, furthermore, they combined the reputation information on direct and indirect. The reputation and trust value were also calculated. This method could effectively isolate the malicious node, but the calculation process was too complex for energy-limited WSNs. There were other representative researches. Janani et al. [20] presented an efficient distributed trust computation with Bayesian and Evidence theorem, on hexagonally clustered MANET.(Mobile Ad hoc NETwork). Mahmud et al. [21] proposed TMM (Trust Management Model) to utilize both node behavioral trust and data trust, which were estimated by using an adaptive neural-fuzzy inference system (ANFIS) including the Beta reputation, and weighted additive methods respectively, to assess the nodes trustworthiness. In addition, Wang et al. [22] used a popular light-weight trust management mechanism–Bayesian trust model. Zhu et al. [23] put forward a rank-based application-driven resilient reputation framework model for wireless sensor networks (RARRM). The model was based on application-driven. The different requirements could rank trust values.

In addition, Umarani et al. [24] established an enhanced Beta trust model (EBTM) to detect malicious attacks. In this model, the neighbor node was selected by the sensor node based on trust information in the course of communication. Moreover, the state of neighbor node was periodically updated. The recovery procedure is incorporated to raise the throughput of the network.

2. Trust management scheme/system

Recently, many researches on trust management schemes were emerging. Within the hierarchical network the cells were divided evenly by grid in plane space, and the data in the cell were processed [18]. Cell distance and number of non-empty cells were defined for processing. And special situations were taken into consideration, such as, the level of trustworthiness about nodes and sleep mode. This mechanism efficiently evaluated reliability of nodes based on the received observations, while DiSLIP (in-network data processing scheme for distributed WSNs) provided efficient performance in detecting nodes that report different events. A secured PKI (Public Key Infrastructure) system [20] was designed by applying the proposed trust management scheme in terms of certificate revocation. By evaluating the hybrid trust value with the trust evaluation vector method, this mechanism was effectively integrated into the hexagonal clusters to secure the PKI framework and detects and classifies the misbehavior, either selfishness or malicious, to take revocation actions on those nodes. Mahmud et al. [21] introduced an ANFIS, brain-inspired TMM to secure IoT devices and relay nodes, and to ensure data reliability. The proposed TMM ensures the function of identifying malicious nodes in the communication network. ETMRM (Energy-efficient Trust Management and Routing Mechanism) [22] firstly extended the sensor flow tables to realize a lightweight trust monitoring and evaluation scheme at the node level, and proposed a centralized trust management scheme to detect and isolate the malicious nodes based on the trust information collected from sensor nodes. Based on game theory, Duan [25] proposed the trust derivation scheme. In this scheme, they analyzed the network security requirements and secure scheme. Then, they established a risk model to stimulate the cooperation of WSNs node to derive an optimal number of cooperating nodes. Finally, the game theoretic approach was applied to the trust scheme derivation process to reduce the overhead of the process. Fang et al. [26] Beta-based Trust and Reputation Evaluation System (BTRES), simulation results show that the use of BTRES could effectively maximize the defense of internal attacks from compromised nodes to improve the WSN information security. Li et al. [27] presented a data-centric trust evaluation mechanism in WSNs (DTSN). They pointed out that WSN was a data-centric network, and the traditional trust evaluation based on entities could not suitable for WSNs. Zia et al. [28] proposed a solution based on communal reputation and individual trust (CRIT) for WSNs. By using watch dog, the nodes' behaviors were monitored, and each node had a trust table and a reputation table for its neighbor nodes.

Fang et al. [29] proposed a trust management scheme to defend against On–Off attack based on Beta distribution. In this scheme, a control factor was introduced to prevent trust value increasing so fast for the malicious node, in order to mitigate the damage of On–Off attack. In Addition, they proposed a Time-window-based Resilient Trust Management Scheme (TRTMS) to defend against the type of attacks [30].

3. Trust-based routing

Wang et al. [22] proposed ETMRM for the software-defined wireless sensor networks. They considered the node's residual energy and trust level to guarantee the transmission of data traffic, to detect the internal network attacks, such as grey hole attacks, black hole attacks, new-flow attacks, efficiently. ETMRM improves the packet delivery ratio, reduces and balances the energy consumption, prolongs the network lifetime, and suffers lower control overhead.

Based on intrusion detection, Gheorghe carried out an Adaptive Trust Management Protocol (ATMP) [31], which was applied in TinyOS system, and it can defend against many kinds of attacks. Fang et al. [32] represented a reputation management scheme. The proposed scheme described the initialization, updating, and storage for the reputation value, as well as the punishment and redemption of malicious nodes. This proposed scheme could apply to the security privacy in sensor network (SPIN) protocol, therefore a novel trust enhanced routing protocol was proposed based on reputation. The simulation indicated that the trust enhanced routing protocol could enhance the security, improve the data forwarding rate and delivery success rate in distrusted environment. Tajeddine et al. [33] put forward a centralized TRust And Competence-based Energy-efficient routing scheme for wireless sensor networks (TRACE). In this scheme, they used centralized management of sinks to make routing more efficient and secure. Subsequently, they proposed a centralized trust-based efficient routing protocol for wireless sensor networks (CENTER) [34]. In the proposed protocol, the BS (Base Station) calculates different quality metrics—namely the maliciousness, cooperation, compatibility and approximates the battery life, which can evaluate the data trust and forwarding trust values of each node. Then, the BS used an effective technique to isolate all "bad" nodes, which is misbehaving or malicious based on their history. At last, the BS uses an efficient method to disseminate updated routing information, indicating the uplinks and the next hop downlink for every node. In addition, Li et al. [35] proposed a novel authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Gerrigagoitia et al. [36] proposed a new IDS design based on reputation and trust of the different nodes of a network for decision-making and analysis of possible sources of malicious attacks. Arijit et al. [37] put forward a trust and reputation based collaborating computing model. The detection of malicious nodes along with trust and reputation analysis of WSN makes this model robust and secure.

The trust management technology has been researched for many years. In distributed networks, the trust generally refers to the trustworthiness of entity. The trust value is a variable, which determines two nodes interact or not. Currently, many scholars focus on how to establish a trust management system, or how to defend against malicious attacks. Unfortunately, they rarely pay attention to the study of trust decision, i.e. how to establish a trust list, or how to select the secure next hop. Hence, we think that trust value is a few measurable metric of security, and we consider the trade-off between energy consumption, minimum hop count and security to propose a novel routing scheme.

In addition, combining fog computer with industrial WSN, we provide a novel applied architecture, namely, F-IWSN. This characteristic of application is lower energy, stronger security and higher transmission performance. Hence, we first propose a Gaussian distribution-based comprehensive trust management system (GDTMS), and then give a trust management-based secure routing scheme (TMSRS) in industrial wireless sensor network with fog computing.

3 TMSRS for F-IWSN

Assuming there is an interaction between node i and node j in the current sensor network environment. The node i calculates the trust value of node j. and then decides whether to interact with it. Firstly, the node i calculates a direct trust value based on historical interaction information with node j. The neighbor node of node j is then queried for the trust value of node j to obtain the indirect trust value of node j and this information is used for trust value integration.

3.1 Initial

The current sensor network environment is assumed that, if there is an interaction between node i and node j. First of all, node i calculates the trust value of node j and then decides whether to interact with it. Moreover, the node i calculates a direct trust value based on historical interaction information with node j. furthermore, it query the common neighbor node of node j to gain the trust value of node j. in order to obtain the indirect trust value of node j, *and* this information is used for trust value integration.

$(a + b)$ times interact between node i and node j, where, a represents the number of successful interactions, and b represents the number of unsuccessful, and obey the Gaussian distribution as follows:

$$N\left(\frac{a}{a+b}, \frac{ab}{(a+b)^2}\right) \tag{1}$$

3.2 Modelling and updating direct reputation

Based on a known set of interactive information, we model Gaussian distribution. The variance is $u^2 = \frac{ab}{(a+b)^2}$, the expectation is given by $v = \frac{a}{(a+b)}$. Assume that the reputation distribution of node i relative to node j is $R_{ij} \sim N(\mu_j, \sigma_j^2)$, $(R_{ij})_1$, $(R_{ij})_2$,…, $(R_{ij})_t$ is the sample of R_{ij} and the parameter of the prior distribution $\mu_{ij} \sim N(v, u^2)$. It is assumed that the reputation is initialized with a Gaussian distribution of N (0.5, 0.25).

3.3 Trust transfer

During the time period t, node i and node j interact $a + b$ times, where a and b are the number of cooperation and non-cooperation, respectively. The conditional density of the parameter μ_j is:

$$p((X_{ij})_1, (X_{ij})_2, \ldots (X_{ij})_t|\mu_j) = \frac{1}{(2\pi)^{\frac{t}{2}}\sigma_j^t}\exp\left(-\frac{\sum_{n=1}^{t}((X_{ij})_n - \mu_j)^2}{2\sigma_j^2}\right) \quad (2)$$

μ_j prior distribution is:

$$\pi(\mu_j) = \frac{1}{\sqrt{2\pi}u}\exp\left(-\frac{(\mu_j - v)^2}{2u^2}\right) \quad (3)$$

Posterior probability density:

$$\pi(\mu_j|(X_{ij})_1, (X_{ij})_2, \ldots, (X_{ij})_t) = \frac{p((X_{ij})_1, (X_{ij})_2, \ldots, (X_{ij})_t|\mu_j)\pi(\mu_j)}{\int_{-\infty}^{+\infty} p((X_{ij})_1, (X_{ij})_2, \ldots, (X_{ij})_t|\mu_j)\pi(\mu_j)d\mu_j} = C\exp(-\frac{(\mu_j - s)^2}{2\eta^2}) \quad (4)$$

$$s = \frac{\frac{t}{\delta_j^2}\overline{X} + \frac{v}{u^2}}{\frac{t}{\delta_j^2} + \frac{v}{u^2}} \quad (5)$$

$$\eta = \frac{1}{\frac{t}{\delta_j^2} + \frac{1}{u^2}} \quad (6)$$

where, C is a constant independent of μ_j. It can be seen that the posterior distribution of μ_j is a Gaussian distribution, so the posterior distribution of the reputation obeys the Gaussian distribution.

3.4 Slot

We assume an average time slot, such as t = 1, 2, 3, 4, 5, 6… When the initial setting is t = 1, the number of success or failures is 1, μ_j = 0.5, σ_j = 0.25, obeying normal distribution of N(0.5, 0.25).

$$A = \frac{t}{0.25}$$
$$B = \frac{(a+b)}{b} \quad (7)$$
$$C = \frac{(a+b)^2}{ab}$$

$\overline{X}$ is ratio, which is the average number of successful interactions for the previous t slots to the total number.

$$DT = s = \frac{A\overline{X} + B}{A + C} \quad (8)$$

For example, when t is 2, X_1 is (1,0), then $\overline{X}=\frac{1+1}{1+1}=1$, yet A = 8, B = 2, C = 9/2, then, DT = 14/17.

3.5 Direct trust

Here, we define the trust value based on the established mathematical model, that is, the mathematical model established based on the number of interactions at the previous moment—the expectation of the Gaussian distribution:

$$DT_{ij} = \text{expectation}\left(\mu_j\right) = s \quad (9)$$

3.6 Aging weight

Historic observations and aging weight in Direct information collected

$$S_{ij}^{new} = \alpha S_{ij} + 1$$
$$U_{ij}^{new} = \beta U_{ij} + 1 \quad (10)$$

where S_{ij} *and* U_{ij} are the number of successful and failed interactions, respectively. α and β are aging weights. Here, the number of successful interactions and the number of failed interactions between S_{ij}^{new} and U_{ij}^{new} at the current moment, Historic observations correspond to *Sij* and *Uij*, plus 1 indicates that the size of the slot is 1 observation.

3.7 Trust decision

The grey theory is a method that focuses on the study of problems involving small samples and bad information. It is often used to make decisions using limited information in Internet applications. The fuzzy set can solve the uncertainty issue, the so-called "qualitative" factor, in the process of the trusted computing process, the gray theory can make the decision of the limited information, the so-called "quantitative" factor. In order to select the most reliable packet forwarding neighbor node, we use grey theory to sort these nodes.

Based on the Grey-based decision making in Ref. [38], we combine the trust management to set the input parameters as follows.

We convert input to the input parameter <Trust Value, Hops>. Since the input of the gray decision is linguistic variables, it is converted into Grey number by combining the actual values [39] to make decisions using Grey-based decision making.

A novel method based on gray likelihood has been proposed to rank candidate preferences in Ref. [40]. This method is suitable for solving group decision problems in an uncertain environment. We assume that $S = \{S_1, S_2, \ldots, S_m\}$ is a set of independent candidates,

$Q = \{Q_1, Q_2, \ldots, Q_n\}$ is a set of n candidate attributes, the attributes are additive and independent, $w = \{w_1, w_2, \ldots, w_n\}$ is the attribute weight vector. In this paper, the attribute weights and ratings of candidate are treated as linguistic variables [40].

The attribute weights are represented by the fractional range of 0–1 shown in Table 1. The attribute rating G is expressed by an integer interval of 0–10 shown in Table 2.

The specific steps are as follows:

1. Determine the attribute weight of the candidate. Assuming that a decision group has K decision makers, the attribute weight of the attribute Q_j can be calculated as:

$$w_j = \frac{1}{k}\left[w_j^1 + w_j^2 + \cdots + w_j^K\right] \tag{11}$$

where, $w_j^K (j = 1, 2, 3, \ldots, n)$ is the attribute weight of the Kth decision maker, and can be described by gray numbers $w_j^K = [\underline{w}_j^k, \overline{w}_j^k]$.

2. Use language variables to rate to get attribute rating values. Then, the rating value G_j can be calculated as

$$G_j = \frac{1}{k}\left[G_{ij}^1 + G_{ij}^2 + \cdots + G_{ij}^K\right] \tag{12}$$

where, $G_{ij}^K (i = 1, 2, \ldots, m; j = 1, 2, \ldots, n)$ is the attribute rating value of the Kth decision maker, and can be described by gray numbers $G_{ij}^K = [\underline{G}_{ij}^k, \overline{G}_{ij}^k]$.

3. Establish a grey decision matrix

$$D = \begin{bmatrix} G_{11} & G_{12} & \cdots & G_{1n} \\ G_{21} & G_{22} & \cdots & G_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ G_{m1} & G_{m2} & \cdots & G_{mn} \end{bmatrix} \tag{13}$$

where, G_{ij} is a linguistic variable based on gray numbers

4. Normalized gray decision matrix

Table 1 Attribute weight range

Range	Weight
Very low (VL)	[0.0, 0.1]
Low (L)	[0.1, 0.3]
Medium low (ML)	[0.3, 0.4]
Medium (M)	[0.4, 0.5]
Medium high (MH)	[0.5, 0.6]
High (H)	[0.6, 0.9]
Very high (VH)	[0.9, 1.0]

Table 2 Attribute evaluation range

Range	Grade
Very poor (VP)	[0, 1]
Poor (P)	[1, 3]
Medium poor (MP)	[3, 4]
Medium (M)	[4, 5]
Medium good (MG)	[5, 6]
Good (G)	[6, 9]
Very good (VG)	[9, 10]

$$D^* = \begin{bmatrix} G_{11}^* & G_{12}^* & \cdots & G_{1n}^* \\ G_{21}^* & G_{22}^* & \cdots & G_{2n}^* \\ \vdots & \vdots & \ddots & \vdots \\ G_{m1}^* & G_{m2}^* & \cdots & G_{mn}^* \end{bmatrix} \tag{14}$$

$$G_{ij}^* = \left[\frac{G_{ij}}{G_j^{\max}}, \frac{\overline{G}_{ij}}{G_j^{\max}}\right] \tag{15}$$

$$G_j^{\max} = \max_{1 \le i \le m}\left\{\overline{G}_{ij}\right\} \tag{16}$$

If the attribute belongs to the cost attribute, the higher the value, the higher the cost paid.

$$G_{ij}^* = \left[\frac{G_j^{\min}}{G_{ij}}, \frac{G_j^{\max}}{\overline{G}_{ij}}\right] \tag{17}$$

$$G_j^{\min} = \min_{1 \le i \le m}\left\{\overline{G}_{ij}\right\} \tag{18}$$

The above normalization method is to retain the attribute of the normalized gray scale range, which is in the range [0, 1].

5. Establish a weighted normalized gray decision matrix. Considering the different importance of each attribute, the weighted normalized gray decision matrix is defined as:

$$D^* = \begin{bmatrix} V_{11}^* & V_{12}^* & \cdots & V_{1n}^* \\ V_{21}^* & V_{22}^* & \cdots & V_{2n}^* \\ \vdots & \vdots & \ddots & \vdots \\ V_{m1}^* & V_{m2}^* & \cdots & V_{mn}^* \end{bmatrix} \tag{19}$$

$$V_{ij} = G_{ij}^* \times w_j \tag{20}$$

6. Use the ideal choice as a reference. For possible candidate scenarios, set to $S = \{S_1, \underline{S}_2, \ldots S_m\}$. The ideal candidate is $S^{\max} = \{G_1^{\max}, G_2^{\max}, \ldots, G_n^{\max}\}$, and it is calculated by:

$$S^{\max} = \left\{ \left[\max_{1 \le i \le m} \underline{V}_{i1}, \max_{1 \le i \le m} \overline{V}_{i1} \right], \left[\max_{1 \le i \le m} \underline{V}_{i2}, \max_{1 \le i \le m} \overline{V}_{i2} \right], \ldots, \left[\max_{1 \le i \le m} \underline{V}_{in}, \max_{1 \le i \le m} \overline{V}_{in} \right] \right\} \quad (21)$$

7. Calculate the degree of gray likelihood between the comparison candidate $S = \{S_1, S_2, \ldots S_m\}$ and the ideal reference candidate S^{max}.

$$\mathrm{P}\{S_i \le S^{\max}\} = \frac{1}{n} \sum_{j=1}^{n} P\left\{ V_{ij} \le G_j^{\max} \right\} \quad (22)$$

8. Arrange the order of candidates. When $P\{S_i \le S^{\max}\}$ is smaller, S_i 's ranking order should be higher, otherwise, the ranking is later.

According to the above procedure, we can determine the ranking order of all candidate paths and choose the best from a set of feasible candidates. A grey-based decision flow chart under multi-path is represented in Fig. 1. The parameters are set in grey-based decision as follows:

Trust Value: trust interval is determined according to the trust value T and the variance Var, $[T - Var, T + Var]$.

Hops: selection of the hop often includes the dynamic change of a certain network topology, hence, the obtained hop A, $[A - 1, A + 1]$ is selected as an input of the gray scale model. Assuming that the hops on the four paths are $Hops\_1$, $Hops\_2$, $Hops\_3$, $Hops\_4$, respectively, the parameters required for the Grey-based decision are positive, that is, the larger the value, the higher the ranking. The hop is exactly the opposite, then after normalization, subtract the resulting normalized value with 1 to get the forward parameter.

Energy selection: for the selection of the next hop node, the energy level can only be taken as a necessary and insufficient condition. When the energy level meets the requirements of the transmission task, it is often more important to consider its trust value (reliability) and dynamic network topology. This is due to that, these two factors often play a more important role in the overall performance of the network. Therefore, when the next hop node is selected, in order to maintain the energy balance of the entire network, the energy levels of all the neighboring nodes are sorted from small to large, and the average energy level is α and the variance is θ. The nodes (at least two nodes) with the first θ*200% are selected for the gray model calculation, and ensure that the node's energy level is not lower than the threshold. The size of the threshold can be set for different transmission loads, default $\alpha - \theta$. Here the energy level is represented by a number between [0, 1], where 1 is the full energy state and 0 is the node dying. A grey decision algorithm under multipath is represented in Table 3.

Table 3 Grey decision algorithm under multipath

Algorithm 1: Grey decision and Energy pre-ranking
Loop
Step 1: according to known dynamic routing protocols, count hops <Hops> for the path to the destination node, to obtain the Residual energy and a Trust value of the current neighbor node.
Step 2: sort all current neighbor energy levels from small to large, The average energy level is α, and the variance is θ. We select the node with θ*200% to calculate the grayscale model, and choose at least two nodes. We ensure that the energy level of the node is not lower than the threshold.
Step 3: Filtered by Step 1, nodes S_1, S_2, …., S_M, Perform Grey-decision calculations. The attributes Q_1 and Q_2 of the node are <Trust value> and <Hops normalized>, respectively. We obtain gray scale sorting results S_1, S_2, …., S_M, prioritize the previous node as the next hop node.
Step 4: jump to Step 1, when data is transferred to the next node.
End arrived at the destination node, the loop ends.

4 Simulation and analysis

In this section, we first compare our proposed GDTMS with RFSN (reputation Beta distribution), then we discuss the TMSRS.

4.1 Gaussian distribution-based trust management scheme

We assume that initial Gaussian reputation distribution is $N(0.5, 0.25)$, α and β are both 0.8, the number of interactions is 30, as each interaction continues successfully or unsuccessfully, then we use MATLAB to simulate. The MATLAB is an advanced technical computing language and interactive environment for algorithm development, data visualization, data analysis, and numerical computing. The trust value changes are shown in Figs. 2 and 3. For continuous cooperation and non-cooperation nodes, the

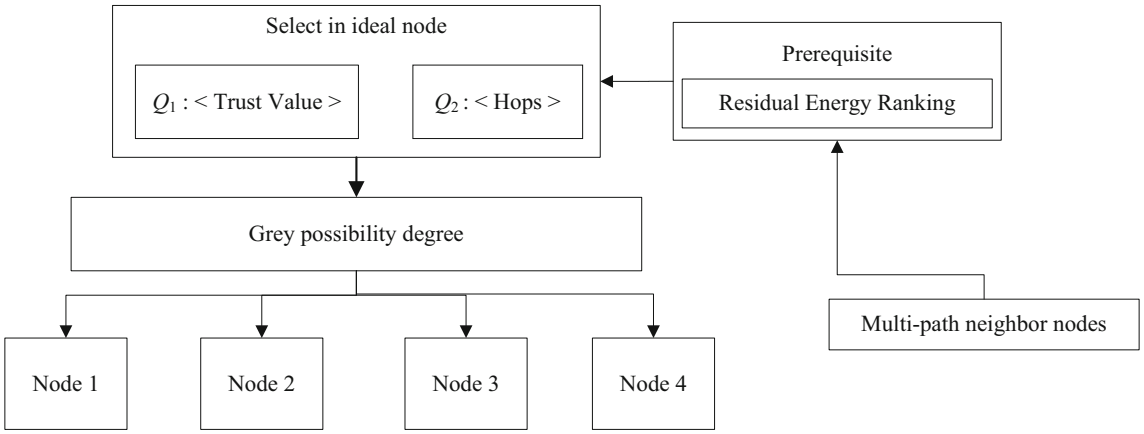


Fig. 1 Grey-based decision flow chart under multi-path

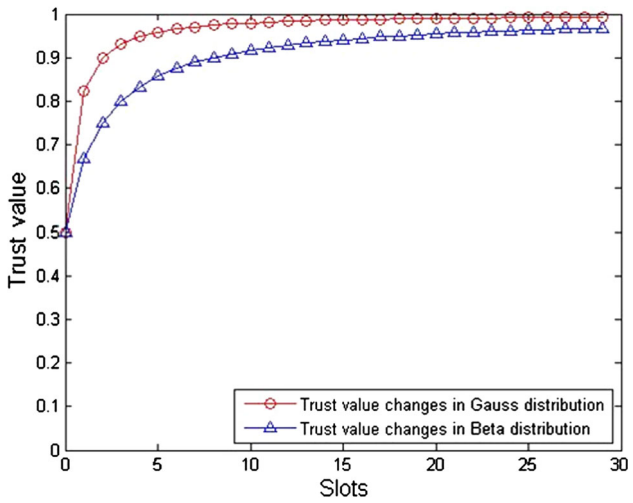


Fig. 2 Comparison of trust value under continuous cooperation

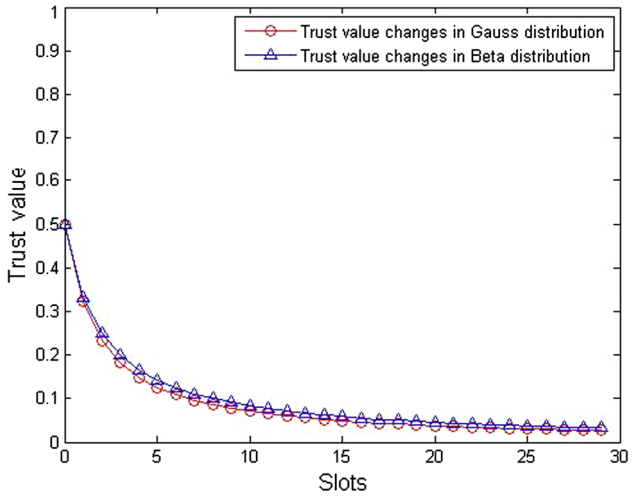


Fig. 3 Comparison of trust value under continuous noncooperation

changes of trust values completely different. They can reflect the trend of change in a timely manner. Comparing with RFSN, the change of trust value for GDTMS tends to highlight the nodes' behavior, hence, GDTMS can applied in the trusted scheme effectively.

From Figs. 2 and 3, if node j and node i continue to cooperate, the trust value continues to rise steadily. Compared with RFSN, The trust value of the Gaussian distribution is stable at around 0.95 after 5 periods, and the former stabilizes at around 0.95 after 25 periods. For a new network, GDTMS is more close to the latest trust compared with RFSN. Similarly, if node j is uncooperative, the GDTMS can still detect them and reduce to the latest reputation.

4.2 Trust management-based energy efficient routing scheme

By using NS-2, which is an object-oriented, discrete event-driven network environment simulator, the improved Grey-based protocol is simulated based on the AODV protocol. Set the network environment as follows, set a transmission node A to send data to the node B, and collect statistics on each type of data packet according to the Trace record file within a certain period of time. The network parameter setting is shown as Fig. 4. The simulated data are compared with the data of AODV [41] and S-ADOV [42] protocols simulated in the same network environment, simultaneously.

The throughput comparison between AODV, Grey-based AODV and SAODV is shown in Fig. 5. In this fugure, the abscissa is the network running time, its unit is s (seconds), the ordinate is the network node throughput, its unit is b/s (bits per second), and its transmission rate is set to 500 b/s.

In the proposed Grey-based AODV, the content of the data packet of the set data packet is reserved for 4 bytes * 3 = 96 bits as the storage trust value, the current remaining energy of the node, and the shortest number of the destination node. Space, respectively, is 4 bytes.

Channel type	Channel/WirelessChannel
Propagation model	Propagation/TwoRayGround
Phy type	Phy/WirelessPhy
Mac protocol type	Mac/802_11
Queue type	Queue/DropTail/PriQueue
Link layer type	LL
Antenna type	Antenna/OmniAntenna
Max packet in queue	50
Routing protocol	AODV
Agent trace	ON
Router trace	ON
Mac trace	ON
Movement trace	ON

Fig. 4 Network parameter setting

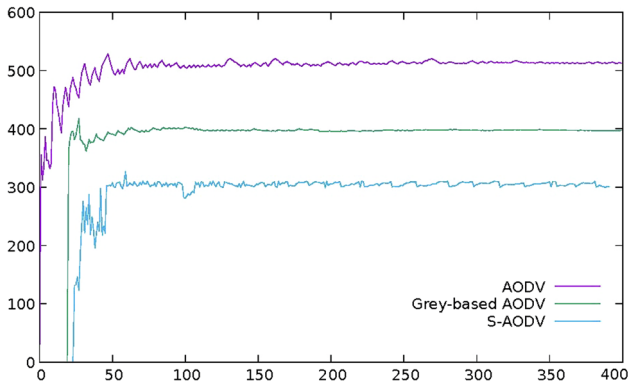


Fig. 5 Throughput comparison between AODV, Grey-based AODV and S-AODV

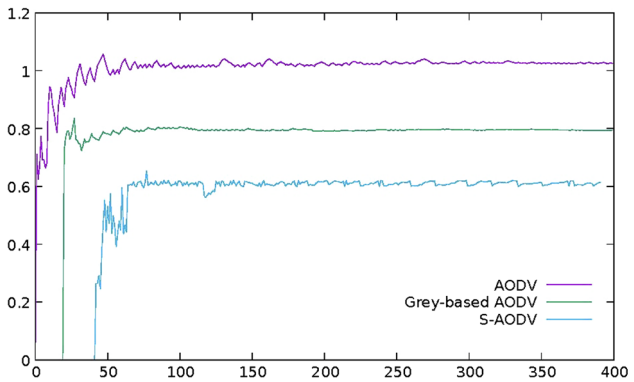


Fig. 6 Energy efficiency comparison between AODV, Grey-based AODV and S-AODV

The energy efficiency comparison between AODV, Grey-based AODV and S-AODV is shown in Fig. 6. In this figure, the ordinate is a numerical ratio, its scope is [0,1]. The abscissa is time, and its unit is second.

$$Energy\_efficiency = \frac{actual\_transimission\_data\_per\_packet}{overall\_transimission\_data\_per\_packet} \quad (23)$$

Similarly, energy efficiency simulation statistics for each transmitted packet. We assume that each transmission of a byte consumes a certain amount of energy, then the actual effective energy ratio can be obtained according to the ratio of the effective data size of the transmission to the total transmission data size. This ratio can reflect the energy efficiency.

The simulation results show that when the trust management mechanism is introduced for decision making, it can still maintain a similar network throughput level with AODV and is superior to S-ADOV. Avoid complex encryption algorithms while maintaining internal network security and ensuring the normal operation of the network.

5 Conclusions

The fog computer can provide real time control and schedule, for industrial wireless sensor network. Unfortunately, the fog-assisted industrial wireless sensor network is still facing many security challenges. Meanwhile, the harsh industrial applications require not only enhanced security, but also high speed transmission performance of information, as well as energy efficiency.

In this paper, our contributions have two parts, and the first is to propose a Gaussian distribution-based comprehensive trust management system (GDTMS). The proposed system could quickly establish the trust management system for normal nodes. The second is to construct secure routing scheme with the trade-off between the security (trust value), energy (residual energy) and transmission (transmission performance). The simulation results show that the proposed TMSRS can meet the security requirement for industrial wireless sensor network.

Acknowledgements Part of this work has been presented at EAI the 2nd EAI International Conference on 5G for Future Wireless Networks (5GWN-2019), Feb 23–24, 2019, Changsha, China [43]. This work is partially supported by the National Natural Science Foundation of China (Nos. 61571004, 51874300), the National Natural Science Foundation of China and Shanxi Provincial People's Government Jointly Funded Project of China for Coal Base and Low Carbon (No. U1510115), the Qing Lan Project, the China Postdoctoral Science Foundation (No. 2013T60574), the Shanghai Natural Science Foundation (No. 17ZR1429100), the Science and Technology Innovation Program of Shanghai (Nos. 115DZ1100400, 17511105903, 17DZ1200302), and the Scientific Instrument Developing Project of the Chinese Academy of Sciences (No. YJKYYQ20170074).

References

1. Wang, H., Shao, L., Li, M., Wang, B., & Wang, P. (2018). Estimation of clock skew for time synchronization based on two-way message exchange mechanism in industrial wireless sensor

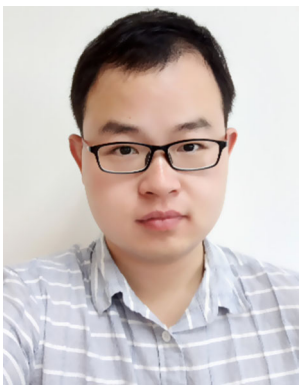
networks. *IEEE Transactions on Industrial Informatics, 14*(11), 4755–4765.
2. Farag, H., Sisinni, E., Gidlund, M., & Österberg, P. (2019). Priority-aware wireless fieldbus protocol for mixed-criticality industrial wireless sensor networks. *IEEE Sensors Journal, 19*(7), 2767–2780.
3. Qin, B., Cai, J., Luo, Y., Zheng, F., Zhang, J., & Luo, Q. (2019). Research and application of intelligent internet of vehicles model based on fog computing. In *IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC)* (pp. 1777–1783).
4. Akram, J., Najam, Z., & Rafi, A. (2018). Efficient resource utilization in cloud-fog environment integrated with smart grids. In *International conference on frontiers of information technology (FIT)* (pp. 188–193).
5. Bukhari, J. F., & Yoon, W. (2018). Design of scalable SDN based eMBMS/WLAN network architecture assisted by fog computing. In *International conference on information and communication technology convergence (ICTC)* (pp. 216–218).
6. Zhu, J., Zou, Y., & Zheng, B. (2017). Physical-layer security and reliability challenges for industrial wireless sensor networks. *IEEE Access, 5,* 5313–5320.
7. Qi, Y., Li, W., Luo, X., & Wang, Q. (2014). *Security analysis of WIA-PA protocol* (Vol. 295, pp. 287–298)., LNEE Berlin: Springer.
8. Mollah, M. B., Vasilakos, A., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications, 84*(C), 34–54.
9. Zou, Y., Zhu, J., Wang, X., & Leung, V. (2014). Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network, 29*(1), 42–48.
10. Sun, L., Ren, P., Du, Q., & Wang, Y. (2016). Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics, 12*(1), 291–300.
11. Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2011). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys and Tutorials, 13*(2), 245–257.
12. Chiwewe, T. M., Mbuya, C. F., & Hancke, G. P. (2015). Using cognitive radio for interference-resistant industrial wireless sensor networks: An overview. *IEEE Transactions on Industrial Informatics, 11*(6), 1466–1481.
13. Zhang, H. J., Xing, H., Nallanathan, Cheng J. A., & Leung, V. C. M. (2016). Secure Resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming. *IEEE Transactions on Industrial Informatics, 12*(10), 1714–1725.
14. Wei, M., Kim, K., Wang, P., & Choe, J. (2011). Research and implementation on the security scheme of industrial wireless network. In *International conference on information networking* (pp. 37–42).
15. Lee, J., Kim, L., & Kwon, T. (2016). FlexiCast: Energy-efficient software integrity checks to build secure industrial wireless active sensor networks. *IEEE Transactions on Industrial Informatics, 12*(1), 6–14.
16. Chen, X., Makki, K., Kang, Y., & Pissinou, N. (2009). Sensor network security: A survey. *IEEE Communications Surveys and Tutorials, 11*(2), 52–73.
17. Ganeriwal, S., & Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. In *The 2nd ACM workshop on security of ad hoc and sensor networks (SASN '04)* (pp. 66–77). Washington, DC, USA: ACM.
18. Firoozi, F., Zadorozhny, V. I., & Li, F. Y. (2018). Subjective logic-based in-network data processing for trust management in collocated and distributed wireless sensor networks. *IEEE Sensors Journal, 18*(15), 6446–6460.
19. Sinha, R. K., & Jagannatham, A. K. (2014). Gaussian trust and reputation for fading MIMO wireless sensor networks. In *International conference on IEEE electronics, computing and communication technologies (CONECCT)* (pp. 1–6). IEEE.
20. Janani, V. S., & Manikandan, M. S. K. (2018). Efficient trust management with Bayesian-evidence theorem to secure public key infrastructure-based mobile ad hoc networks. *Eurasip Journal on Wireless Communications and Networking, 1,* 25.
21. Mahmud, M., Kaiser, M. S., Rahman, M. M., Rahman, M. A., Shabut, A., Al-Mamun, S., et al. (2018). A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications. *Cognitive Computation, 10*(5), 864–873.
22. Wang, R., Zhang, Z., Zhang, Z., & Jia, Z. (2018). ETMRM: An energy-efficient trust management and routing mechanism for SDWSNs. *Computer Networks, 139*(5), 119–135.
23. Zhu, M., Chen, H., & Wu, H. (2010). A rank-based application-driven resilient reputation framework model for wireless sensor networks. In *International conference on computer application and system modeling (ICCASM)* (pp. V9-125–V9-129). IEEE.
24. Labraoui, N. (2015). A reliable trust management scheme in wireless sensor networks. In *12th international symposium on programming and systems (ISPS)* (pp. 1–6).
25. Duan, J., Gao, D., Yang, D., Foh, C. H., & Chen, H.-H. (2014). An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. *IEEE Internet of Things Journal, 1*(1), 58–69.
26. Fang, W., Zhang, C., Shi, Z., Zhao, Q., & Shan, L. (2016). BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks. *Journal of Network and Computer Applications, 59*(1), 88–94.
27. Li, M., Hu, J., & Du, J. (2010). A data-centric trust evaluation mechanism in wireless sensor networks. In *The 9th international symposium on distributed computing and applications to business engineering and science (DCABES)* (pp. 466–470). IEEE.
28. Zia, T. A., & Islam, M. Z. (2010). Communal reputation and individual trust (CRIT) in wireless sensor networks. In *International conference on availability, reliability, and security (ARES'10)* (pp. 347–352). IEEE.
29. Fang, W., Shi, Z., Shan, L., Li, F., & Wang, X. (2015). Trusted scheme for defending on-off attack based on BETA distribution. *Journal of System Simulation, 27*(11), 2722–2728.
30. Fang, W., Zhang, W., Yang, Y., Liu, Y., & Chen, W. (2017). A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution. *Science China Information Sciences, 60*(4), 040305.
31. Gheorghe, L., Rughinis, R., & Tataroiu, R. (2013). Adaptive trust management protocol based on intrusion detection for wireless sensor networks. In *Proceedings of networking in education and research, 2013 RoEduNet international conference 12th Edition* (pp. 1–7). IEEE.
32. Fang, F., Li, J., & Li, J. (2013). A reputation management scheme based on multi-factor in WSNs. In *International conference on mechatronic sciences, electric engineering and computer* (pp. 3843–3848). IEEE.
33. Tajeddine, A., Kayssi, A., & Chehab, A. (2011). TRACE: A centralized trust and competence-based energy-efficient routing scheme for wireless sensor networks. In *The 7th international wireless communications and mobile computing conference (IWCMC)* (pp. 953–958). IEEE.
34. Tajeddine, A., Kayssi, A., & Chehab, A. (2012). CENTER: A centralized trust-based efficient routing protocol for wireless sensor networks. In *The 10th annual international conference on privacy, security and trust* (pp. 195–202). IEEE.

35. Li, X., Niu, J., Kumari, S., Liao, J., Liang, W., & Khan, M. K. (2016). A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. *Security and Communication Networks, 9*(15), 2643–2655.
36. Gerrigagoitia, K., Uribeetxeberria, R. U., & et al. (2012). Reputation-based intrusion detection system for wireless sensor networks. In *Complexity in engineering* (pp. 1–5). IEEE.
37. Arijit, U. (2010). Trust and reputation based collaborating computing in wireless sensor networks. In *The 2nd international conference on computational intelligence, modelling and simulation* (pp. 464–469). IEEE.
38. Li, G. D., Yamaguchi, D., & Nagai, M. (2007). A grey-based decision-making approach to the supplier selection problem. *Mathematical and Computer Modelling, 46*(3), 573–581.
39. Arce, M. E., Saavedra, Á., Míguez, J. L., et al. (2015). The use of grey-based methods in multi-criteria decision analysis for the evaluation of sustainable energy systems: A review. *Renewable and Sustainable Energy Reviews, 47,* 924–932.
40. Wang, S. J., & Hu, H. A. (2005). Application of rough set on supplier's determination. In *The 3rd annual conference on uncertainty* (pp. 256–262).
41. Perkins, C. E., & Royer, E. M. (1999). Ad hoc on-demand distance vector routing. In *The 2nd workshop on mobile computing systems and applications (WMCSA)* (pp. 90–100).
42. Guerrero, M. (2001). Secure ad hoc on-demand distance vector (SAODV) routing. INTERNETDRAFT draft-guerrero-manet-saodv-00.txt.
43. Fang, W., Zhang, W., Chen, W., Liu, Y., & Tang, C. (2019). TME^{2}R: Trust management-based energy efficient routing scheme in fog-assisted industrial wireless sensor network. In *The 2nd EAI international conference on 5G for future wireless networks (5GWN-2019)*, Feb 23–24, 2018, Changsha, China: EAI (to be published).

Weidong Fang 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 China University of Mining and Technology, Beijing, in 1998, and the Ph.D. degree in Electromagnetic Fields and Microwave Techniques from Shanghai University, Shanghai, in 2016. Now, he is serving as an Associate Professor in Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai, China. Currently, his research interests are energy efficiency and cyber security in wireless sensor network, including trust management, secure network coding and secure routing protocol.

Wuxiong Zhang 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 Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai, in 2013. He is currently an Associate Professor with SIMIT and is serving as an associate professor with the Shanghai Research Center for Wireless Communications. His research interests include beyond third-generation mobile communication systems and vehicular networks.

Wei Chen received the B.Eng. degree in Medical Imaging and the M.S. degree in Paleontology and Stratigraphy from China University of Mining and Technology, Xuzhou, China, in 2001 and 2005, respectively, and the Ph.D. degree in Communications and Information Systems from China University of Mining and Technology, Beijing, China, in 2008. In 2008, he joined the School of Computer Science and Technology, China University of Mining and Technology, where he is currently a Professor. He is a Member of IEEE. His research interests include machine learning, image processing, computer networks and wireless communications.



Yang Liu received the B.E. degree in Microelectronics from Anhui University, Hefei, China, in 2012, and the M.E. degree in Software Engineering from Beijing University of Aeronautics and Astronautics, in 2016. He is currently a Ph.D. candidate in Communication and Information System at Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, Shanghai. His current research interests include mobile computing, Internet of Things, and wireless localization.

Chaogang Tang received the B.S. degree from the Nanjing University of Aeronautics and Astronautics in 2007 and the Ph.D. degree from the School of Information Science and Technology, University of Science and Technology of China in 2012. He is currently a Lecturer with the China University of Mining and Technology. His research interests include mobile cloud computing, fog computing, Internet of Things, big data, and WSN.