TME^{2}R: Trust Management-Based Energy Efficient Routing Scheme in Fog-Assisted Industrial Wireless Sensor Network

Weidong Fang[1,2], Wuxiong Zhang[1,2], Wei Chen[3(✉)], Yang Liu[1,2], and Chaogang Tang[3]

[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
chenw@cumt.edu.cn

Abstract. Fog-assisted Industrial Wireless Sensor Network (F-IWSN) is a novel wireless sensor network (WSN) in the industry. It not only can more efficiently reduce information transmission latency, but also can more conducively achieve real-time control and rapid resource scheduling. However, similar to other distributed networks, it also faces enormous security challenges, especially from 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 analytic hierarchy process 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, Trust Management-based Energy Efficient Routing Scheme (TME^{2}R). In addition, GDTMS is 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 · Fog computing · Secure routing protocol · Trust management

1 Introduction

As the next-generation broadband 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 smartphones - it also supports a variety of smart

V. C. M. Leung et al. (Eds.): 5GWN 2019, LNICST 278, pp. 155–173, 2019.
https://doi.org/10.1007/978-3-030-17513-9_11

terminals. In the past few years, with the 5G networks development, industrial wireless sensor network (IWSN) have been successfully deployed in industrial fields, such for safety protection, production supervision, data acquisition, and control etc. 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 IssS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service). It has provided many opportunities 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, field 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 and services to the edge of the network. Similar to Cloud, Fog provides computational, networking and storage services to terminal-users. In a sense, fog computing is also a paradigm of 5G flat management. However, different from Cloud, the fog provides additional advantages such as distributed characters, which is the key feature of the fog computing.

Due to its distributed feature, fog computing enable providing services outside the cloud, at the edge of the network and closer to terminal devices., It has several technical innovations with the following aspects: (1) Storage, (2) Communication, (3) Control, configuration, measurement and management. Compared with some previous technologies, such as storing data primarily in cloud data centers, routing over the internet backbone, controlling primarily by network gateways (i.e. those gateways in the LTE core network), fog computing can use one or more collaborative terminal-user clients or near-user edge devices to carry out a substantial amount of storage, communication, control, configuration, measurement and management. Hence, it can provide low latency, location awareness, and improved quality-of-services (QoS) for streaming and real time applications, as well as the real time big data analytics. It also supports densely distributed data collection. Fog computing is well positioned for many application scenarios: it is strongly useful in connecting vehicle, smart grid and wireless sensor and actuator networks (WSAN) [3]; it has great potential in smart building and software-defined networking (SDN) [4]. Moreover, the augmented reality (AR) and real-time video analytics, the content delivery and caching, and the mobile big data analytics also benefit from concept of fog computing [5]. In a word, the fog computing is introduced into IWSN, namely fog-assisted Industrial Wireless Sensor Network (F-IWSN). A typical architecture of F-IWSN is shown in Fig. 1.

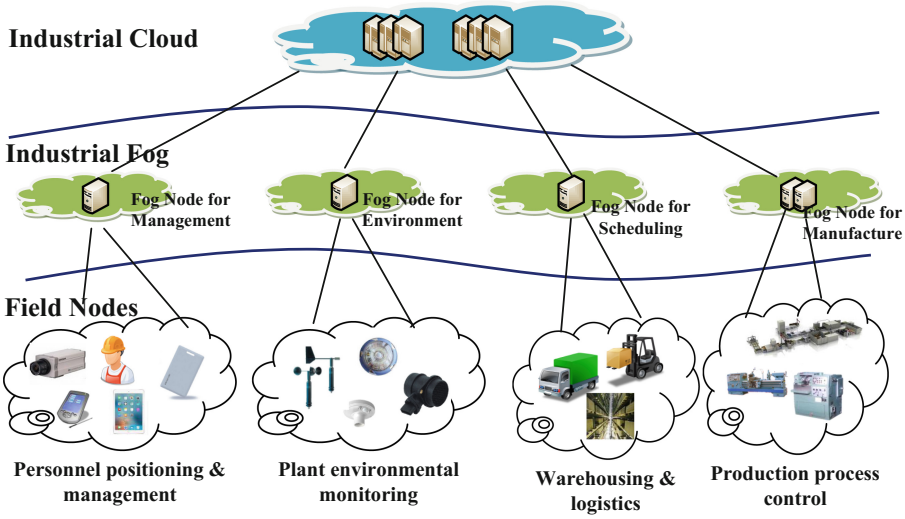

Fig. 1. A typical fog-based IWSN architecture

Practically, just as classical IWSN, 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 reduce 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 IWSN. Many technologies are researched to meet the above requirements of IWSN. Currently, there are three accepted standards: Wireless HART [6], International Society of Automation (ISA) 100.11a [7], and WIA-PA [8]. The Wireless HART is a mesh network which utilizes the time-division multiple access (TDMA) to transmit data packets and route them by using graph routing. The ISA100.11a uses TDMA with variable time-slot, and transmitted paths are made by the graph routing and source routing. The 6LoWPAN is utilized to provide the advantage of Internet protocol (IP) into the wireless system. The WIA-PA supports the hybrid topology of star and mesh, and it exploits hybrid mode of CDMA and CSMA. All of them use IEEE 802.15.4 standard at PHY and MAC layer under the 2.4-GHz frequency spectrum.

Compared with the wireless sensor network (WSN), F-IWSN not only has stronger security requirements, but also face more security challenges. F-IWSN needs to detect the malicious nodes quickly, and defend against it effectively, when the network is invaded or attacked. The harsh deployed environments lead to the obvious degradation of the wireless channel quality, which increases the packet loss rate. Hence, it is very difficult to distinguish between the normal noise and the jamming attacks [9], especially, those internal attacks (i.e. Black hole attack, selective forwarding attack, and tampering attack). In addition, once these unauthorized nodes access 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, involving encryption and authentication, can guarantee the content security. However, it cannot defend against the internal attacks. Meanwhile, more and more researches show that the trust management scheme is an effective technology to defend against the internal attack. Hereby, a novel trust management scheme based on binomial distribution is proposed to defend against On-Off 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 countermeasures in IWSN are discussed, and the detection and defense schemes against On-Off attack are reviewed. The Binomial Distribution-based Trust Management Scheme (GDTMS) for F-IWSN is proposed, especially Trust Management-based Energy Efficient Routing Scheme (TME^{2}R) 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 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 sensed information 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 [10]. This is due to that the broadcast characteristic and openness of the wireless medium, IWSN is vulnerable to be eavesdropped [9].

Traffic Analysis: an attacker can obtain the source and destination node addresses and route by monitoring and analyzing PDUs, and further deduce the network topology

and routing algorithm to launch the tamper attack. Also because of the openness nature 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 sensor node and sink nodes in IWSN. Since 2.4 GHz is usually facilitated in IWSN, the attacker can launch this attack to interference the network using Wi-Fi or Bluetooth devices which are under the same frequency spectrum.

Power exhaustion attack [11]: 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 the 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: any DoS attacks can cause IWSN not to provide services properly. There are two 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 CRC, 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.

(1) *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, utilized by the above mentioned three standards, 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 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-byte sub-strings. One of the 16-byte sub-strings are set to calculate 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-byte 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 transportation 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 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 [9]. 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 [10]. 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 [12]. Sun et al. [13] 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 [14], 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. [15] proposed and integrated cognitive radio technique into IWSNs to enhance the detection and defense ability for the interference. Zhang et al. [16] 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 [17]. 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. proposed FlexiCast [18], 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 [19], 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. proposed the reputation-based framework for high integrity sensor networks (RFSN) [20]. Then, based on Beta distribution and Bayesian formula, the Beta reputation system for sensor networks (BRSN) was proposed. BRSN is a simple trust evaluation system and it has been widely studied and used. Firoozi et al. still follows the classical trust model Beta reputation, use time windows to subdivide time slot in a hierarchical network, and the trust values of different clusters are averaged and normalized. [21]. Sinha proposed the Gaussian trust and reputation for fading MIMO WSNs [22]. 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 are also calculated. This method can effectively isolate the malicious node, but the calculation process is too complex for energy-limited WSNs. There are other representative researches. Janani et, al. presents an efficient distributed trust computation with Bayesian and Evidence theorem, on hexagonally clustered MANET [23]. Mahmud et al., proposed TMM to utilize both node behavioral trust and data trust, which are estimated using ANFIS including the Beta reputation, and weighted additive methods respectively, to assess the nodes trustworthiness [24]. In addition, Wang et al. used a popular light-weight trust management mechanism–Bayesian trust model [25]. Zhu et al. [26] put forward a rank-based application-driven resilient reputation framework model for wireless sensor networks (RARRM). The model is based on application-driven. The different requirements could rank trust values.

Umarani et al. established enhanced beta trust model (EBTM) to detect malicious attacks [27]. 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 is 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 are emerging. Within the hierarchical network the cells were divided evenly by grid in plane space, and the data in the cell were processed [21]. Cell distance and number of non-empty cells were defined for processing. And special situations into consideration, such as, the level of trustworthiness about nodes and sleep mode. This mechanism efficiently assesses reliability of nodes based on the received observations, while DiSLIP provides efficient performance in detecting nodes that report different events. A secured PKI system [23] is designed in the paper 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 is 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 [24] et al. introduced an adaptive neuro-fuzzy inference system (ANFIS). Brain-inspired trust management model (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 [25] firstly extend the Sensor Flow tables to realize a

lightweight trust monitoring and evaluation scheme at the node level and propose 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 [28] 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. Beta-based Trust and Reputation Evaluation System (BTRES) [29], 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. [30] 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. [31] 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. proposed a trust management scheme to defend against On-Off attack based on BETA distribution [32]. 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 h proposed a time-window-based resilient trust management scheme (TRTMS) to defend against the type of attacks [33].

3. TRUST-BASED ROUTING

Wang proposed - An Energy-efficient Trust Management and Routing Mechanism (ETMRM) [25] for SDWSNs proposed the ETMRM-An Energy-efficient Trust Routing Mechanism for SDWSNs, considering the node's residual energy and trust level to guarantee the transmission of data traffic, detecting the internal network attacks, such as Greyhole attacks, Blackhole 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) [34], which is applied in TinyOS system, and it can defend against many kinds of attacks Fang et al. represented a reputation management scheme [35]. 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. put forward a centralized TRust And Competence-based Energy-efficient routing scheme for wireless sensor networks (TRACE) [36]. 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) [37]. 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 proposed a novel authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity [38]. Gerrigagoitia 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 [39]. Arijit 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 had been researched for many years. In distributed networks, the trust generally refers to the trustworthiness of entity. The trust value is unusually a variable. It 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. Moreover, we argue that trust value is a few measurable metric of security.

Otherwise, joint fog computer and industrial WSN provide a novel applied architecture. 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 energy efficient routing (TME^{2}R) scheme in Fog-assisted Industrial Wireless Sensor Network.

3 TME^{2}R for Fog-Assisted Industrial Wireless Sensor Network

Assume there is an interaction between node *i* and node *j* in the current sensor network environment; Node *i* calculates the trust value of node *j*. and then decides whether to interact with it. First, 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* calculate 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 $u^2 = \frac{ab}{(a+b)^2}$ is expectation is given by $v = \frac{a}{(a+b)}$. Assume that the reputation distribution of node i relative to node j is $R_{ij} \sim \mathrm{N}(\mu_\mathrm{j}, \sigma_\mathrm{j}^2)$, $(R_{ij})1$, $(R_{\mathrm{ij}})2$, …, $(R_{\mathrm{ij}})\mathrm{t}$ is the sample of $\mathrm{R_{ij}}$ and the parameter of the prior distribution $\mu_{\mathrm{ij}} \sim \mathrm{N}(v, u^2)$. 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:

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

μ_j prior distribution is:

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

Posterior probability density:

$$\begin{aligned} &\pi(\mu_j|(X_{ij})_1, (X_{ij})_2, \cdots, (X_{ij})_t) \\ &= \frac{p((X_{ij})_1, (X_{ij})_2, \cdots, (X_{ij})_t|\mu_j)\pi(\mu_j)}{\int_{-\infty}^{+\infty} p((X_{ij})_1, (X_{ij})_2, \cdots, (X_{ij})_t|\mu_j)\pi(\mu_j)d\mu_j} \\ &= C\exp\left(-\frac{(\mu_j - s)^2}{2\eta^2}\right) \end{aligned} \tag{4}$$

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

$$\eta = \frac{1}{\frac{t}{\delta_j^2} + \frac{1}{u^2}} \tag{6}$$

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 $t = 1, 2, 3, 4, 5, 6\ldots$ When the initial setting is $t = 1$, the number of success or failures is 1, $\mu j = 0.5$, $\sigma j = 0.25$, obeying normal distribution of $N(0.5, 0.25)$.

$$\begin{aligned} A &= \frac{t}{0.25} \\ B &= \frac{(a+b)}{b} \\ C &= \frac{(a+b)^2}{ab} \end{aligned} \tag{7}$$

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

$$\mathrm{DT} = s = \frac{A\overline{X} + B}{A + \mathrm{C}} \tag{8}$$

For example, when t is 2, $X1$ 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:

$$DT_{ij} = \mathrm{expectation}\left(\mu_j\right) = s \tag{9}$$

3.6 Aging Weight

Historic observations & Aging weight in Direct information collected

$$\begin{aligned} \mathrm{S}_{ij}^{new} &= \alpha S_{ij} + 1 \\ U_{ij}^{new} &= \beta U_{ij} + 1 \end{aligned} \tag{10}$$

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 Sij^{new} and Uij^{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

As the only security quantitative indicator, Trust value can have multiple security purposes, such as removing malicious nodes out of trusted table, or canceling it convergence role. However, for Industrial WSN, especially Fog-assisted Industrial WSN, they need secure and efficient transmission, meanwhile, reduce energy consumption.

Hence, based on our previous research, we introduce the multi-dimensions Analytic Hierarchy Process (AHP)

AHP <Trust Value, Energy, Hops, QoS, ToS)>

Where, QoS (Quality of Service) involves more data metric of the transmission layer, such as packet loss rate, and latency. ToS (type of service): in the network layer, the data types transmitted are divided into three categories: text, audio, and video, which are assigned three different priorities of low, medium, and high. All above, full consideration of the actual needs of network transmission represents (Fig. 2).

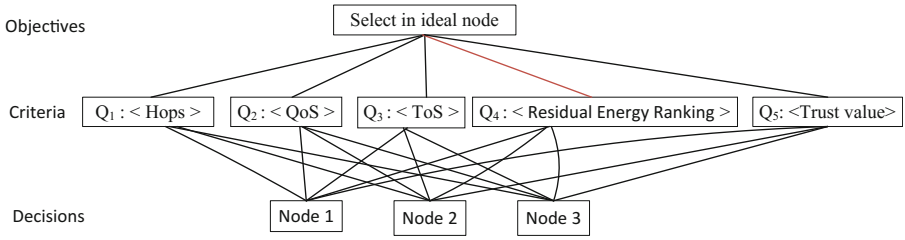

Fig. 2. A trust-based AHP

4 Simulation and Analysis

In this section, we first compare our proposed GDTMS with RFSN (reputation Beta distribution), then we discuss the TME^{2}R routing scheme.

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 trust value changes as shown: For continuous cooperation and non-cooperation nodes, the 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.

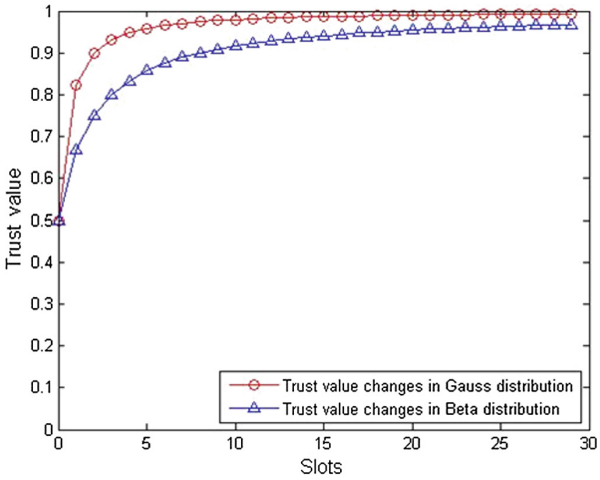

Fig. 3. Comparison of trust value under continuous cooperation

From Figs. 3 and 4, 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.

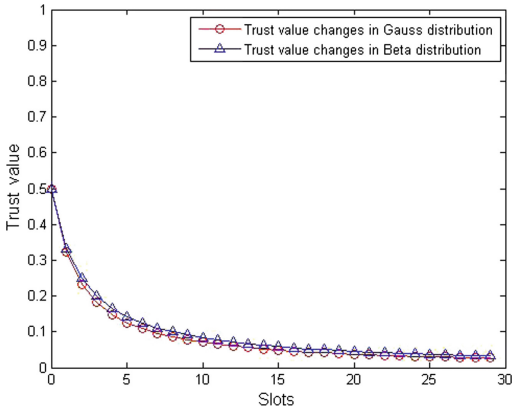

Fig. 4. Comparison of trust value under continuous noncooperation

4.2 Trust Management-Based Energy Efficient Routing Scheme

By using NS2, the improved AHP-based protocol based on the AODV protocol is simulated, in which a certain transmission node A is set to send data to the node B, and

each type of data packet is counted according to the Trace record file within a certain period of time. The specific parameters are set as follows.

The above parameters, the abscissa is the network running time, its unit is s (seconds), the ordinate is the network throughput, its unit is b/s (bits per second), and the network transmission rate is set to 500 bits/s. In the proposed AHP-based AODV in this paper, the content of the data packet of the set data packet is reserved for 3 Bytes * 5 = 120 bits as the storage trust value, the current remaining energy of the node, and the destination node. The shortest hop count, end-to-end delay, network transmission data type and other five parameters of the memory space, respectively, is 3 bytes (Fig. 5).

$$Throughput = \frac{actual\_transimission\_data}{overall\_transimission\_data\_packet} \times transimission\_rate \tag{11}$$

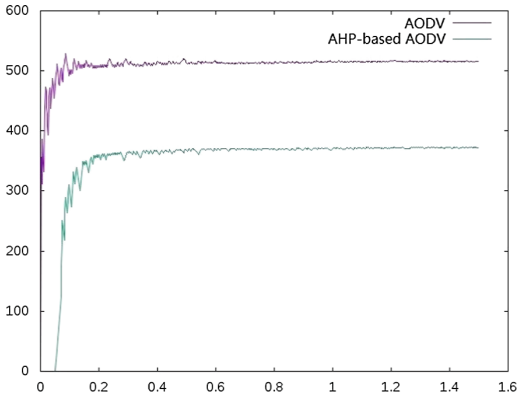

Fig. 5. Throughput

Here, the throughput simulation removes those data packet, which involve the routing establishment and routing maintains, and the routing overhead. Meanwhile, this simulation also removes the five parameters of the AHP-based routing protocol, including storing the trust value, the node's current remaining energy, the required reach of the destination node, as well as actual effective data transmission rate under the condition of the shortest hop count, end-to-end latency. Finally, it represents the network transmission data type (Fig. 6).

$$Energy\_efficiency = \frac{actual\_transimission\_data\_per\_packet}{overall\_transimission\_data\_per\_packet} \tag{12}$$

Similarly, energy efficiency simulation, statistics for each transmitted packet, assuming that each bit of actual transmission 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. To reflect the effectiveness of energy.

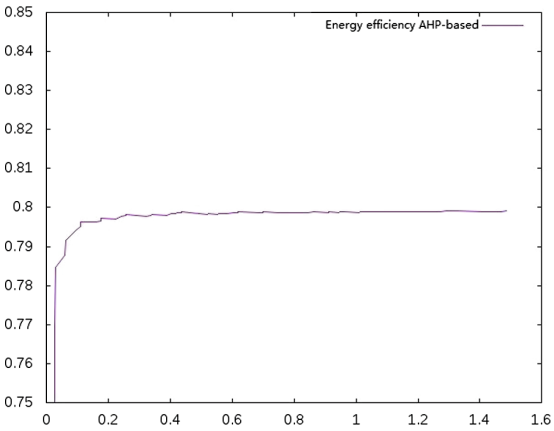

Fig. 6. Energy efficiency.

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 higher speed transmission performance of information, as well as energy efficiency.

In this paper, our contributions have two parts, 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 the trade-off between the security (trust value), energy (residual energy) and transmission (transmission performance). The trade-off can meet the security requirement for industrial wireless sensor network.

Acknowledgment. Part of this work has been presented at IEEE 18th International Conference on Computer and Information Technology (CIT-2018), July 30 - Aug 03, 2018, Halifax, Canada, [41] This work is partially supported by the National Natural Science Foundation of China (61571004), the Shanghai Natural Science Foundation (No. 17ZR1429100), the Science and Technology Innovation Program of Shanghai (No. 115DZ1100400, No. 17511105903, No. 17DZ1200302), the Scientific Instrument Developing Project of the Chinese Academy of Sciences (No. YJKYYQ20170074) and Fujian Science and Technology Plan STS Program (2017T3009).

References

1. Gungor, V.C., Hancke, G.P.: Industrial wireless sensor networks: challenges, design principles, and technical approaches. IEEE Trans. Ind. Electron. **56**(10), 4258–4265 (2009)
2. Salam, H.A., Khan, B.M.: IWSN - standards, challenges and future. IEEE Potentials **35**(2), 9–16 (2016)

3. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the 1st Edition the MCC Workshop on Mobile Cloud Computing, pp. 13–16 (2012)
4. Stojmenovic, I., Wen, S.: The fog computing paradigm: scenarios and security issues. Comput. Sci. Inf. Syst. **2**, 1–8 (2014)
5. Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R.H., Morrow, M.J., Polakos, P.A.: A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges. arXiv preprint arXiv: 1710.11001 (2017)
6. Song, J., Han, S., Mok, A.K., Chen, D., Lucas, M., Nixon, M.: WirelessHART: applying wireless technology in real-time industrial process control. In: Proceedings of Real-Time and Embedded Technology and Applications Symposium, pp. 377–386. IEEE (2008)
7. Rezha, F.P., Shin, S.Y.: Performance analysis of ISA100.11a under interference from an IEEE 802.11b wireless network. IEEE Trans. Ind. Electron. **10**(2), 919–927 (2014)
8. Liang, W., Zhang, X., Xiao, Y., Wang, F., Zeng, P., Yu, H.: Survey and experiments of WIA-PA specification of industrial wireless network. Wirel. Commun. Mob. Comput. **11**(8), 1197–1212 (2011)
9. Zhu, J., Zou, Y., Zheng, B.: Physical-layer security and reliability challenges for industrial wireless sensor networks. IEEE Access. **5**, 5313–5320 (2017)
10. Qi, Y., Li, W., Luo, X., Wang, Q.: Security analysis of WIA-PA protocol. In: Wang, X., Cui, L., Guo, Z. (eds.) Advanced Technologies in Ad Hoc and Sensor Networks. LNEE, vol. 295, pp. 287–298. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54174-2_26
11. Mollah, M.B., Azad, M.A.K., Vasilakos, A.: Security and privacy challenges in mobile cloud computing: survey and way ahead. J. Netw. Comput. Appl. **84**, 34–54 (2017)
12. Zou, Y., Zhu, J., Wang, X., Leung, V.: Improving physical-layer security in wireless communications using diversity techniques. IEEE Network **29**(1), 42–48 (2014)
13. Sun, L., Ren, P., Du, Q., Wang, Y.: Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. IEEE Trans. Ind. Electron. **12**(1), 291–300 (2016)
14. Pelechrinis, K., Iliofotou, M., Krishnamurthy, S.V.: Denial of service attacks in wireless networks: the case of jammers. IEEE Commun. Sur. **13**(2), 245–257 (2011)
15. Chiwewe, T.M., Mbuya, C.F., Hancke, G.P.: Using cognitive radio for interference-resistant industrial wireless sensor networks: an overview. IEEE Trans. Ind. Electron. **11**(6), 1466–1481 (2015)
16. Zhang, H.J., Xing, H., Cheng, J., Nallanathan, A., Leung, V.C.M.: Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming. IEEE Trans. Ind. Inform. **12**(10), 1714–1725 (2016)
17. Wei, M., Kim, K., Wang, P., Choe, J.: Research and implementation on the security scheme of industrial wireless network. In: Proceedings of International Conference on Information Networking, pp. 37–42 (2011)
18. Lee, J., Kim, L., Kwon, T.: FlexiCast: energy-efficient software integrity checks to build secure industrial wireless active sensor networks. IEEE Trans. Ind. Inform. **12**(1), 6–14 (2016)
19. Chen, X., Makki, K., Kang, Y., Pissinou, N.: Sensor network security: a survey. IEEE Commun. Sur. **11**(2), 52–73 (2009)
20. Ganeriwal, S., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In: Proceedings of the 2nd ACM workshop on Security of ad Hoc and Sensor Networks (SASN 2004), pp. 66–77. ACM, Washington, D.C. (2004)
21. Firoozi, F., Zadorozhny, V.I., Li, F.Y.: Subjective logic-based in-network data processing for trust management in collocated and distributed wireless sensor networks. IEEE Sens. J. **18**(15), 6446–6460 (2018)

22. Sinha, R.K., Jagannatham, A.K.: Gaussian trust and reputation for fading MIMO wireless sensor networks. In: Proceedings of IEEE International Conference on IEEE Electronics, Computing and Communication Technologies (CONECCT) pp. 1–6 (2014)
23. Janani, V.S., Manikandan, M.S.K.: Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks. Eurasip J. Wirel. Commun. Networking **1**, 25 (2018)
24. Mahmud, M., Kaiser, M.S., Rahman, M.M., et al.: A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications. Cogn. Comput. (9), 1–10 (2018)
25. Wang, R., Zhang, Z., Zhang, Z., Jia, Z.: ETMRM: an energy-efficient trust management and routing mechanism for SDWSNs. Comput. Netw. **139**, 119–135 (2018)
26. Zhu, M., Chen, H., Wu, H.: A rank-based application-driven resilient reputation framework model for wireless sensor networks. In: Proceedings of International Conference on IEEE Computer Application and System Modeling (ICCASM), vol. 9, pp. V9-125–V9-129 (2010)
27. Labraoui, N.: A reliable trust management scheme in wireless sensor networks. In: IEEE International Symposium Programming System, pp. 1–6 (2015)
28. Duan, J., Gao, D., Yang, D., et al.: An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. IEEE Internet Things J. **1**(1), 58–69 (2014)
29. Fang, W., Zhang, C., Shi, Z., Zhao, Q., Shan, L.: BTRES: beta-based trust and reputation evaluation system for wireless sensor networks. J. Network Comput. Appl. **59**(1), 88–94 (2017)
30. Li, M., Hu, J., Du, J.: A data-centric trust evaluation mechanism in wireless sensor networks. In: 2010 Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), pp. 466–470. IEEE (2010)
31. Zia, T.A., Islam, M.Z.: Communal reputation and individual trust (CRIT) in wireless sensor networks. In: Proceedings of IEEE International Conference on Availability, Reliability, and Security (ARES 2010), pp. 347–352 (2010)
32. Fang, W., Shi, Z., Shan, L., Li, F., Wang, X.: Trusted scheme for defending on-off attack based on BETA distribution. J. Syst. Simul. **27**(11), 2722–2728 (2015)
33. Fang, W., Zhang, W., Yang, Y., Liu, Y., Chen, W.: A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution. Sci. Chin. Inform. Sci. **60**(4), 040305 (2017)
34. Gheorghe, L., Rughinis, R., Tataroiu, R.: Adaptive trust management protocol based on intrusion detection for wireless sensor networks. In: 2013 RoEduNet International Conference 12th Edition Proceedings of Networking in Education and Research, pp. 1–7. IEEE (2013)
35. Fang, F., Li, J., Li, J.: A reputation management scheme based on multi-factor in WSNs. In: Proceedings of IEEE International Conference on Mechatronic Sciences, Electric Engineering and Computer, pp. 3843–3848 (2013)
36. Tajeddine, A., Kayssi, A., Chehab, A.: TRACE: a centralized trust and competence-based energy-efficient routing scheme for wireless sensor networks. In: Proceedings of the 7th IEEE International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 953–958 (2011)
37. Tajeddine, A., Kayssi, A., Chehab, A.: CENTER: a centralized trust-based efficient routing protocol for wireless sensor networks. In: Proceedings of IEEE Tenth Annual International Conference on Privacy, Security and Trust, pp. 195–202 (2012)
38. Li, X., Niu, J., Kumari, S., Liao, J., Liang, W., Khan, M.K.: A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Secur. Commun. Networks **9**(15), 2643–2655 (2016)

39. Gerrigagoitia, K., Uribeetxeberria, R., Zurutuza, U., et al.: Reputation-based intrusion detection system for wireless sensor networks. In: Proceedings of IEEE Complexity in Engineering, pp. 1–5 (2012)
40. Arijit, U.: Trust and reputation based collaborating computing in wireless sensor networks. In: Proc of the Second IEEE International Conference on Computational Intelligence, Modelling and Simulation, pp. 464–469 (2010)
41. Zhou, N., Fang, W., Zhang, W., Lv, X., Huang, J.: A novel trust management scheme for defending against On-off attack based on Gaussian distribution. In: Proceedings of IEEE 18th International Conference on Computer and Information Technology (CIT-2018), July 30 - Aug 03, 2018, Halifax, Canada, to be published