Journal of Artificial Intelligence and Technology, 2022, 2, 23-31
https://doi.org/10.37965/jait.2021.12004

ISTP
RESEARCH ARTICLE

A Data Transmission Approach Based on Ant Colony Optimization and Threshold Proxy Re-encryption in WSNs

Jing Liu,[1,2] Zenghui Liu,[3] Chenyu Sun,[1] and Junxi Zhuang[1]

[1]College of Computer Science, Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
[2]Engineering Research Center of Intelligent Perception and Autonomous Control, Ministry of Education, Beijing 100124, China
[3]College of Automation Engineering, Beijing Polytechnic, Beijing 100176, China

(Received 13 December 2020; Revised 23 December 2021; Accepted 23 December 2021; Published online 27 December 2021)

Abstract: Wireless sensor networks (WSNs) have become increasingly popular due to the rapid growth of the Internet of Things. As open wireless transmission media are easy to attack, security is one of the primary design concerns for WSNs. Current solutions consider routing and data encryption as two isolated issues, providing incomplete security. Therefore, in this paper, we divide the WSN communication process into a data path selection phase and a data encryption phase. We propose an improved transmission method based on ant colony optimization (ACO) and threshold proxy re-encryption for WSNs, and we named it as ACOTPRE. The method resists internal and external attacks and ensures safe and efficient data transmission. In the data path selection stage, the ACO algorithm is used for network routing. The improvement of the pheromone concentration is proposed. In order to resist attacks from external attackers, proxy re-encryption is extended to WSN in the data encryption stage. The threshold secret sharing algorithm is introduced to generate a set of re-encryption key fragments composed of random numbers at the source node. We confirm the performance of our model via simulation studies.

Keywords: wireless sensors network; ant colony optimization; pheromone; proxy re-encryption; threshold

I. INTRODUCTION

The Internet of Things (IoT) is expanding rapidly, reaching several domains including personal health care, environmental monitoring, home automation, smart mobility, and Industry 4.0 [1,2]. The report of Industry Revolution 4.0 by Juniper Research predicted that the total number of Industrial IoT sensors in use will increase from 17·7 billion in 2020 to 36·8 billion in 2025, representing an overall growth rate of 107% [3]. Wireless sensor networks (WSNs) are a core technology that can provide a large volume of heterogeneous data from the long-term observation of large-scale scenarios [4]. The main objective of sensor networks is to sense the environment and send information to a base station for further communication and processing [5].

The main challenges associated with WSNs are network security, load balancing, and network life cycle. WSNs are usually deployed in unsupervised and insecure environments, and their nodes can be attacked and destroyed by malicious attackers. Attackers can also use compromised sensor nodes to disrupt communications or insert misleading sensor data. Furthermore, sensors are generally powered by energy-constrained batteries and have limited computational ability. These challenges must be considered and addressed while designing WSN protocols. Therefore, it is vital to detect faults and enhance the overall performance of the network by monitoring network activities, minimizing risk, and ensuring that network activities, such as data gathering and data processing, can be performed without interruption.

Several studies and surveys have been conducted [6–10] to address the security concerns associated with WSNs. However, existing security methods are limited to a certain stage of transmission and balancing the trade-off between improving the transmission performance of WSNs and data security. In this study, we improve a data transmission method based on ant colony optimization (ACO) and threshold proxy re-encryption to defend against internal and external attacks from the data path selection phase and the data encryption phase, which method can find a suitable trade-off way between security and network performance. The path selection phase approach in the ACOTPRE is based on ACO and can determine an optimal route from source to destination through the continuous accumulation and updating of pheromones. Data security is achieved by a proxy re-encryption-based threshold algorithm that uses intermediate nodes to protect data from malicious attackers. In addition, we also compare the simulation results of ACOTPRE with those of AODV (Ad hoc On-Demand Distance Vector Routing) and ReTE-AODV (refined trust energy ad hoc on demand distance vector routing algorithm) [11]. The main contributions of this study are

- Aiming at internal attackers, this paper improves a data path selection scheme based on ACO. This paper proposes to reconstruct the pheromone concentration factor, including trust evaluation model, residual energy model, and node signal strength. When selecting the next hop node, it fully considers the impact of internal attacks, network energy consumption, and transmission link quality. It is proposed to improve the pheromone update strategy, considering the average and minimum node energy. Compared with the traditional ant colony

Corresponding author: Zenghui Liu (e-mail: 100150@bpi.edu.cn).

algorithm, the improved scheme fully considers the characteristics and requirements of WSNs.

- Aiming at external attackers, this paper improves a data encryption scheme based on proxy re-encryption. The source node uses Lagrangian interpolation polynomials to construct the re-encryption key fragments and distribute them to the proxy node. The destination node calculates the Lagrange interpolation polynomial recovers the symmetric key. According to the threat model proposed by the characteristics of WSNs, the corresponding security analysis is carried out.
- The simulation experiment compares the ReTE-AODV and AODV protocols and evaluates the performance of packet delivery ratio (PDR), end-to-end delay (EED), and average residual energy (ARE). The simulation results show that the ACOTPRE scheme sacrifices some transmission time and energy consumption to ensure secure data transmission, but PDR is increased by 19% and 22%, respectively.

The rest of this paper is organized as follows: in Section II, we present a brief review of related work; in Section III, we describe ACOTPRE architecture, first presenting the routing protocol and then explaining the use of proxy re-encryption in WSNs; in Section IV, we perform simulation experiments to evaluate the performance of the proposed approach and discuss the results of the experiments; finally, we conclude the paper in Section V.

II. RELATED WORK

This section investigates and analyzes existing methods for enhancing security in WSN environments. Some of these methods aim to enhance the security of the routing phase, whereas others focus on data security.

A. ROUTING PROTOCOL IN WSN

Due to the open medium and dynamic entry of new nodes in WSNs, routing protocols must establish trust relationships to avoid malicious nodes [12]. *Pirzada et al.* [13] proposed a trust-based routing protocol, wherein trust agents obtain trust levels from events that are directly experienced by the nodes. The trust values of all subsequent hops in the path are compared and the hop with the highest trust value is selected. The trust–distrust protocol (TDP) [14] is divided into four phases. The fitness calculated in the second phase of the link quality assessment is used as the trust parameter in the third phase. In the fourth stage, path selection is performed based on the ranking of the trust capabilities of the nodes. The energy of sensor nodes is limited and must be considered while designing routing protocols. A novel Metric-based RPL (Routing Protocol for Low-power and Lossy Networks) Trustworthiness Scheme (MRTS) was proposed in ref. [15], combining selfishness, honesty, ETX, and four energy parameters to evaluate the credibility of a node. The MRTS can be adjusted by adding or deleting behavior combinations for specific IoT applications. The self-channel observation trust and reputation system (SCOTRES) [12] is another novel trust management scheme that integrates with the DSR (Dynamic Source Routing). It is assessed by direct and indirect knowledge and includes four metrics in the direct assessment. However, it differs from previous schemes as it includes channel health metrics, which provide tolerance for periodic failures due to bad channel conditions and protects the network from jamming attacks. ReTE-AODV was introduced in ref. [11] using Bayesian probability for trust management, owing to its ability to handle uncertainty while obtaining a refined form of the trust calculation, allowing it to select a reliable route that consumes low energy and sends packets in a trustworthy manner.

Cryptography can also be used in WSNs. A secure routing algorithm based on energy optimization (EOSR) [16] can improve the security of a route by distributing a public–private key pair before deployment. The secure identity-based routing protocol [17] introduces node identity authentication to ensure the security of network routing and prevent witch attacks and wormhole attacks. The elliptical curve encryption algorithm is used for the route discovery process to ensure that the nodes discovered are credible. This protocol also uses an energy threshold to ensure that the nodes do not consume excessive energy. Sreevidya *et al*. [18] proposed the use of an ACO algorithm to identify the formation of cluster nodes in mobile sensor networks, designate cluster head nodes, and establish routes using the AODVRP routing protocol and the Diffie-Hellman Key exchange (DHKE) algorithm to achieve safe data transmission and reduce the number of nodes and the overhead of storing public keys.

B. PROXY RE-ENCRYPTION

The concept of proxy re-encryption was first proposed by Blaze *et al*. in 1998 [19]. Subsequently, Ateneses *et al*. [20] proposed the first one-way proxy re-encryption scheme. The proxy was given a re-encryption key that could convert Alice's ciphertext to Bob's ciphertext without understanding the message encrypted under any key. Currently, proxy re-encryption is widely used as a tool in encrypted data storage and data sharing to protect the confidentiality of data stored with third parties, such as electronic health records, cloud computing, and digital rights management. Due to its relevancy, it has been utilized in identity-based PRE schemes [21,22], wherein the user's public key is regarded as their identity. However, the scheme proposed in ref. [22] still faces the threat of collusion. Consequently, a one-way threshold proxy re-encryption scheme was applied to the blockchain in ref. [23], which solved the problem wherein the use of a centralized CA for identity verification can result in hidden safety hazards when a new node starts to communicate with nodes in the blockchain network.

The SHIB-PRE scheme [24] proposed a new concept for WSNs of proxy re-encryption of the source hidden identity, which supports the gateway in the wireless network to directly transfer the encrypted data of one user to another. The underlying plaintext data is disclosed throughout the sharing stage, but the agent must be a gateway or cloud.

The scheme proposed in ref. [25] is a conditional proxy broadcast re-encryption scheme that supports regular release but does not provide flexible encryption and complete security certification. A time and ID-based agent re-encryption scheme was proposed in ref. [26] that does not require any trust in the agent but adds a time element so that the sender can further divide the message into fine molecules based on the specified time period to provide agents with more fine-grained re-encryption capabilities. The timed-release proxy conditional re-encryption scheme [27] is a more flexible encryption method. In addition to ensuring the privacy of user files under the constraints of time factors, each user can freely communicate with another user to share files. The recipient does not obtain any information regarding the file until the specified time.

Reference [28] presented a data security re-encryption scheme based on the trusted authorization that takes advantage of the performance required for re-encryption tasks within the cloud. Trusted authorities are only responsible for key regeneration,

thereby achieving efficient and scalable security. In the VANET (vehicular ad hoc network) scenario, Kanchan *et al*. [29] presented a technique which group signatures are combined with non-transit proxy re-encryption technology to enhance the security and effectiveness of messages sent over the network without requiring multiple re-transmissions. This algorithm uses the bilinear Diffie–Hellman method, which cannot be easily broken by opponents. It can manage keys and decryption rights using agents and PKG, respectively, thereby reducing the workload of the member manager. A multi-agent proxy re-encryption scheme [30] was constructed using proxy re-encryption and re-splittable threshold passwords in the grid, but each ciphertext fragment in the scheme requires verification, which would inevitably lead to significant computational overheads and reduce the scalability of the system.

The above analysis demonstrates that insecurity can be easily introduced into the network due to the characteristics of the WSN, and that existing security methods are limited to achieving a balance between improving the transmission performance of the WSN and data security. The method proposed herein performs these tasks in coordination, thereby improving the overall performance. ACOTPRE is a WSN data transmission method based on ACO and proxy re-encryption, including the data path selection phase and data encryption transmission phase. A reliable routing protocol is required to provide complete security during both these phases. For the path selection method based on the ACO algorithm, the optimal path for data transmission from the source to the destination can be determined through the continuous accumulation and updating of pheromones. Data security is realized by using a proxy re-encryption algorithm for the intermediate node to prevent malicious attackers from accessing the data, thereby enabling the safe sharing of the final data.

III. ACOTPRE ARCHITECTURE

This section presents a framework of ACO and proxy re-encryption algorithms to improve WSNs considering two common problems —optimal path selection and reliable data transmission.

A. DATA PATH SELECTION PHASE

1) SYSTEM MODEL AND ASSUMPTIONS. The network monitoring area is assumed to be a circle. A total of N sensor nodes are randomly distributed inside the circle and the base station is located at the apex of the network monitoring area. In addition, making the following assumptions: 1) once deployed in the network, sensor nodes do not move coordinates and correspond to a unique coordinate position and ID identification. 2) Each node in the network acts as both the source node and the forwarding node, and the base station only serves as the destination node. 3) The base station has enough energy, and the other node has the same initial energy. The topology of this WSN is shown in Fig. 1.

2) ROUTING ALGORITHM DESIGN. The problem of secure routing in WSNs is a combinatorial optimization problem, wherein the data of each node can be transmitted to other nodes more reasonably. The ACO algorithm is a metaheuristic algorithm for combinatorial optimization problems and can be used to solve complex dynamic combinatorial optimization problems to improve network security and prolong the life cycle of the network. To design a safe and efficient routing algorithm, we introduce the node trust model, energy consumption, and signal strength of the node into the ant colony algorithm, as pheromone concentration

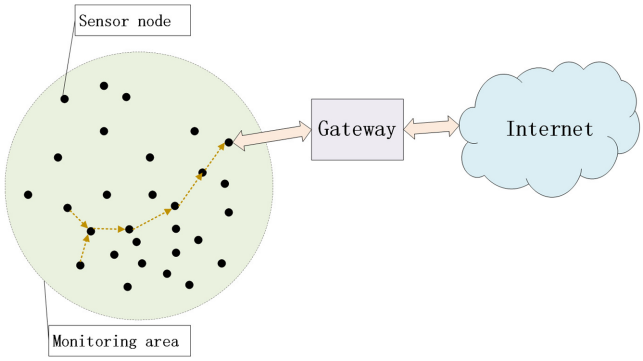

Fig. 1. Topology of the WSN.

factors. At a time t, each ant selects a path for the proposed improvement of the ACO algorithm, as indicated by the probabilistic formula:

$$P_{ij}^{n}=\begin{cases}\frac{[H_{ij}(t)]^{\alpha}\cdot[\eta_{ij}(t)]^{\beta}}{\sum_{S\subset allowed_s}[H_{is}(t)]^{\alpha}\cdot[\eta_{is}(t)]^{\beta}}, & s\subset allowed_s\\ 0, & \text{other}\end{cases} \tag{1}$$

The influence of the pheromone concentration H and the distance on message propagation are simultaneously considered during routing, and $H(t)$ represents the pheromone at the time t. The heuristic function $\eta(t)=\frac{1}{(d_{ik}+d_{kj})}$,$d_{ik}=[(x_i-x_k)^2+(y_i-y_k)^2]^{\frac{1}{2}}$ denotes the distance between the source node i and the intermediate node k, and $d_{kj}=[(x_k-x_j)^2+(y_k-y_j)^2]^{\frac{1}{2}}$ represents the distance between the intermediate node k and the destination node j. The impact factors α and β control the influence of the pheromone intensity and heuristic information, respectively.

C) CALCULATION OF PHEROMONE. The first pheromone factor is a node trust model, which includes the direct trust and the indirect trust, to detect the interaction behavior of each node. The trust degree of a node is an indicator of the security of the node and remains in the interval [0,1]. Normal nodes can easily participate in excessive route discovery while implementing security measures, thereby consuming the available energy in a short period of time, exiting the network prematurely, and affecting the quality of communication. Therefore, we propose calculations for the energy percentage and link quality to improve the stability of data transmission.

Trust Model: A trust model essentially performs trust derivation, computation, and application [13]. Trust evaluation in a routing procedure is an assessment of the forwarding behavior of neighbors by a sender. In this study, we analyze the behavior of receiving and forwarding packets and the characteristics of the monitoring capability of neighbor nodes considering the following: 1) packet contents may be too large; 2) the number of packets is too large, which may result in a denial of service attack; and 3) the node does not forward packets or modify content forwarding. Two indexes, namely, the packet content repetition rate and the packet number, are chosen as evaluation parameters. The direct and indirect trusts of the node are determined by adopting an appropriate trust model and weighting each trust to obtain a comprehensive trust value for each node. The comprehensive trust value is introduced into the ant colony algorithm as one of the pheromone concentration factors.

As stated, the indicators are determined considering two aspects—packet content repetition rate and the number of packets [31]. The direct trust can be defined as a vector $(T_{ij}^{D})'$:

$$(T_{ij}^{D})' = \{R_{ij}(t), N_{ij}(t)\} \tag{2}$$

where $R_{ij}(t)$ is the packet content repetition rate and $N_{ij}(t)$ is the number of data packets. The specific measurement formula is

$$\begin{cases} R_{ij}(t) = e^{n_{ij}(t) - rn_{ij}(t)} \\ N_{ij}(t) = e^{-|n_{ij}(t) - \Delta n_{ij}(t)|} \end{cases} \tag{3}$$

where $n_{ij}(t)$ is the number of data packet transmissions at a time t, $rn_{ij}(t)$ is the number of data packet transmission repetitions, and $\Delta n_{ij}(t)$ is the expected value of data packet transmissions. These factors have different proportions for different application requirements, and the weighted average method can be used to calculate the direct trust of node i and node j. Here, the weight is represented by the vector W:

$$W = \{w_R, w_N\}^T \tag{4}$$

where $0 < w_R, w_N < 1$ and $w_R + w_N = 1$. Therefore, the direct trust of the actual node is $T_{ij}^{D} = (T_{ij}^{D})'W$. Once the network node is initialized, the initial direct trust $T_{ij}^{D} = \{0,1\}$ as node i and node j do not interact. The node update cycle is Δt. Once the update cycle is reached, the node responds to dynamic changes in real time and updates the direct trust.

Indirect trust T_{ij}^{I} is calculated by the feedback evaluation value provided by the neighbor node, and it cannot recommend the received recommendation information from one node to another. The indirect trust T_{ij}^{I} may incur additional communication costs for trust exchange. To simplify the trust model, only the history of direct interactions between nodes is used to compute trust. In this way, the iteration of trust value transmission can be avoided. The direct and indirect trust between nodes is shown in Fig. 2.

Assuming that there are $k_1, k_2 \ldots k_n$ nodes between node i and node j, $T_{i,k_1}^{D}, T_{i,k_2}^{D} \ldots T_{i,k_n}^{D}$ can be defined as the direct trust of node i with respect to node $k_1, k_2 \ldots k_n$. Similarly, $T_{k_1,j}^{D}, T_{k_2,j}^{D} \ldots T_{k_n,j}^{D}$ can be defined as the direct trust of node $k_1, k_2 \ldots k_n$ to node j with respect to node j:

$$T_{ij}^{I} = \frac{\sum T_{i,k}^{D} T_{k,j}^{D}}{\sum T_{i,j}^{D}} \tag{5}$$

Comprehensive trust T_{ij} is given by the linear combination of direct trust and indirect trust:

$$T_{ij} = (1 - \omega) T_{ij}^{D} + \omega T_{ij}^{I} \tag{6}$$

where ω represents the weight of indirect trust. In many trust evaluation models proposed at present, the weight value is set as a fixed value according to the preference of direct trust and indirect trust in different scenarios. Then, when a node in the network fails, the value of trust will change greatly in a certain period of time. Therefore, this paper introduces the coefficient of variation to reflect the change of direct and indirect trust. Then the weight calculation formula is as follows:

$$\omega = \frac{V_{T_{ij}^{D}}}{V_{T_{ij}^{D}} + V_{T_{ij}^{I}}} \tag{7}$$

where V is the coefficient of variation and $V = \sigma/\rho$, where σ is the standard deviation of trust and ρ is the average trust. When the coefficient of variation is smaller, it indicates a more stable degree of trust change. For example, if the coefficient of variation increases for a large change in direct trust, then the weight of indirect trust also increases, and a more stable indirect trust is preferred in the weighting.

Residual Energy: Sensor nodes are usually severely constrained in terms of their computing power. The energy consumption can be defined in the process of sending and receiving data packets. The residual energy Er of the node can be calculated as:

$$E_c = (P_t + P_r) \cdot \frac{D_s}{D_r} \tag{8}$$

$$E_r = E_{\text{all}} - E_c \tag{9}$$

The energy factor is calculated as $E = E_r / E_{\text{all}}$, and its value is between [0,1]. P_t is the transmission power, D_s is the size of the data packet, D_r is the packet transmission rate, P_r is the received power, and E_c is the energy consumed by node i to transmit the data packet to node j. E_{all} is the initial energy and is included in the data packet of the node.

Signal Strength: When the distance between nodes is large, the signal strength is poor and the transmission can be affected by noise and interference, resulting in packet loss. To ensure that the routing protocol can provide stable data transmission, the parameter p is introduced as the reference standard for communication link evaluation in the WSN. It indicates the strength and quality of the received data packets. The node signal strength is calculated based on the TwoRayGround transmission model as:

$$p = \frac{P_t \cdot G_t \cdot G_r \cdot h_t^2 \cdot h_r^2}{d^4 \cdot L} \tag{10}$$

where P_t is the transmitted power, G_t is the antenna gain of the sending node, G_r is the antenna gain of the receiving node, h_t is the height of the transmitting antenna, h_r is the height of the receiving antenna, d is the distance between two nodes, and L is the system loss factor.

Pheromone Concentration: Once the pheromone concentration influencing factors have been calculated, we can calculate the pheromone concentration H as:

$$H = \alpha_1 T + \alpha_2 E + \alpha_3 p \tag{11}$$

where α is the coefficient of each factor, and $\alpha_1 + \alpha_2 + \alpha_3 = 1$.

Pheromone update: The ants in the basic ant colony algorithm reach the destination through the path with the most pheromones. If a path is the optimal path to the destination, several ants pass through it, significantly decreasing the energy of the network node on the path, and reducing the life cycle of the entire network. Therefore, when considering pheromone updates, ants must be able to pay attention to the changes in path energy and path length to determine the optimal path. When the energy of different path

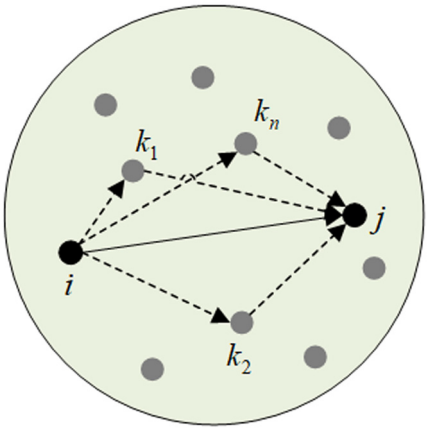

Fig. 2. Direct and indirect trust assessment diagram.

lengths is the same, the shortest path must be chosen as the optimal path. Considering the minimum energy and the AE of the path nodes, we can effectively balance the energy load of the network and reduce the energy gap between nodes to avoid the death of some of the nodes on a path due to energy exhaustion. The global information update rules of the ant colony algorithm proposed herein are

$$H_{ij}(t+1) = (1-\rho)H_{ij}(t) + \Delta H_{ij}^{n} \tag{12}$$

The ant week model is used as the pheromone local update algorithm model. The improved formula is

$$\Delta H_{ij}^{n}(t+1) = \frac{E_{n(min)}}{E_{n(avg)}} \cdot \frac{Q}{L_k} \tag{13}$$

where $E_{n(min)}$ and $E_{n(avg)}$ represent the minimum energy and average energy, respectively, of an ant n passing through the path nodes; L_n denotes the path length taken by an ant n from the source node to the destination node; and Q is a globally set constant.

4) ROUTE MAINTENANCE. The pheromone concentration H is updated for each node at intervals of time t. As the message spreads, two trends appear in the link:

- When the trust of the nodes in a link is relatively stable, most of the messages will pass through the path with the highest trust. Due to the forwarding of several messages, the energy of the nodes along this path decreases. When this happens, the weight assigned to the energy in the calculation of the pheromone concentration H will increase for the nodes with lower energy. Consequently, the H of the low-energy nodes reduces, and other paths with a higher transition probability are selected. Thus, the energy load of the entire network can be balanced, thereby improving the energy efficiency of the network.
- When the trust of the nodes in a link is unstable, based on the trend of slow increase and decrease in trust, the trust of the node will decrease. The weight of the corresponding trust will increase significantly, thereby reducing the value of H; for example, when a node in a link does not perform the corresponding operation. Subsequently, the nodes with a higher transition probability will be determined. Notably, uncooperative nodes can be determined quickly and the current path can be changed if it contains uncooperative nodes.

B. DATA ENCRYPTION PHASE

To counter external attackers, this paper introduces proxy re-encryption into the wireless network environment. The proxy re-encryption algorithm is introduced in the data encryption phase to provide technical support for data security assurance. The sensor nodes communicate with each other through a multi-hop wireless link, and the intermediate nodes in the network responsible for forwarding are the proxy nodes. These proxy nodes convert the received ciphertext and send it correctly to the destination node, and the specific scheme is designed as follows.

1) PRELIMINARIES. In this section, we provide the necessary preliminary details.

Bilinear Map: G and G_T denote two multiplicative cyclic groups with the same prime order q. g is a generator of group G. A bilinear pairing is a bilinear map $e: G \times G \rightarrow G_T$.

Notation: The notation used in this scheme are

a. H_2: hash functions, $G^2 \rightarrow Z_q$.

b. H_3: hash functions, $G^3 \rightarrow Z_q$.

c. H_4: hash functions, $G^3 \times z_q \rightarrow Z_q$.

d. H_5: Key derivation function, $G \rightarrow \{0,1\}^l$.

Protocol: As with most PRE schemes, the protocol has a total of seven phases: Setup, KeyGen, SymKeyGen, Encrypt, ReEncrypt, ReDecrypt, and Decrypt.

2) PROPOSED SCHEMES. This paper gives a data encryption scheme using proxy re-encryption based on a gated secret sharing scheme using Lagrangian polynomials, the security of which relies on the discrete logarithm difficulty problem. The source node encrypts the data information to be transmitted using a symmetric encryption algorithm and later constructs multiple re-encryption keys by polynomial interpolation in the gated secret sharing algorithm, allowing the proxy node to transform the symmetrically encrypted ciphertext of the source node into a ciphertext that can only be decrypted by the private key of the destination node, and the specific scheme design is shown in Fig. 3.

Set public parameters: The global public parameter is tuple: $params = (G,g,H_2,H_3,H_4,H_5)$. The global common parameters are shared by all the participants in the WSN.

Key generation algorithm: The source node contains its own key pair generation algorithm and a proxy re-encryption key generation algorithm, and also by default both the source and destination nodes have access to each other's public keys.

(a) *KeyGen(params)*: randomly select $a,b \in Z_q$, calculate g^a, g^b and generate a key pair $(pk_A,sk_A) = (g^a,a)$, $(pk_B,sk_B) = (g^b,b)$.

(b) *ReKeyGen*(sk_A,pk_B,N,k): Enter the key $sk_A = a$, $pk_B = g^b$. N fragments (representing the N proxy node), whose threshold is k, which implies that at least k proxy nodes are required to decrypt the proxy re-encryption:

- Randomly select $x_A \in Z_q$ and calculate $X_A = g^{x_A}$.
- Calculate $d = H_3(X_A,pk_B,(pk_b)^{x_A})$ and $D = H_3(pk_A,pk_B,(pk_B)^a)$, where d is the Diffie–Hellman of B's key pair and temporary key pair (x_A,X_A), the result of the key exchange. This shared key is used to make the re-encryption key of the scheme noninteractive.
- Randomly select of $k-1$ $S_i \in Z_q$, where $1 \le i \le k-1$, and calculate $S_0 = a \cdot d^{-1} modq$. Construct the polynomial $S(x) \in Z_q$, similar to $S(x) = S_0 + S_1 x + S_2 x^2 + \ldots + S_{k-1} x^{k-1}$.
- Select random number $id \in Z_q$, calculate $s_x = H_2(id,D)$, calculate polynomial $c = S(s_x)$, $\sigma_1 = H_4(id,pk_A,pk_B,X_A)$ and $\sigma_2 = a \cdot \sigma_1$. Define the re-encryption key fragment $regen_frag$ as a tuple $(id,rk,X_A,\sigma_1,\sigma_2)$,where σ_1 and σ_2 are the signatures of the re-encrypted key fragments.
- Repeat N times and output a set of re-encrypted key fragments $regen_frag$.The source node distributes the re-encryption key fragment $regen_frag$ to each proxy node.

SymKeyGen (pk_A): When pk_A is entered, selecting random number $e,u \in Z_q$, and calculating $E = g^e, U = g^u$, and $s = u + E \cdot H_2(E,U)$, we will get the tuple $C = (E,U,s)$. After checking the validity, the symmetric key $K = H_5((pk_A)^{e+u})$ is calculated through the key derivation function.

Encrypt(K,C,M): The symmetric key K obtained by the *SymKeyGen* algorithm is used to symmetrically encrypt the message M to obtain $encM$, and the cipher text $C_1 = (encM,C)$ is output. This ciphertext is the first layer of the ciphertext and be sent by the source node to each proxy node.

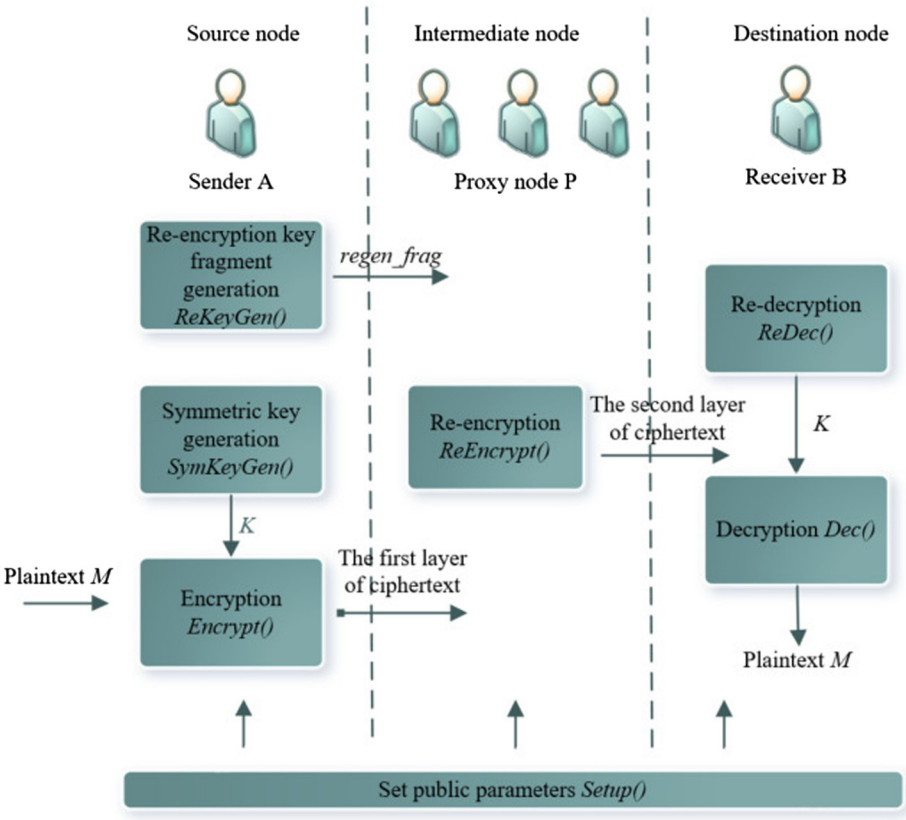

Fig. 3. Proxy re-encryption scheme works.

$ReEncrypt(regen_frag,C_1)$: After receiving the re-encryption key fragment and the first layer of cipher text, the proxy node re-encrypts the first layer of cipher text. First, the $encM$ in C_1 is kept unchanged. Then, calculate $E_1 = E^c$ and $U_1 = U^c$. Finally, the second layer key fragment $C_frag = (E_1,U_1,id,X_A)$ is output, and the second layer of ciphertext $C_P = (encM,C_frag)$ is obtained.

$ReDecrypt(sk_B,pk_A,C_{P_{i=1}}^k)$: The destination node must receive the $C_{P_{i=1}}^k$ of k proxies to decrypt the ciphertext.

- First, enter the private key of destination node and the public key of source node, then we will get $C_frag_{i=1}^k = (E_{1,i},U_{1,i},id_i,X_A)$ from proxy nodes.
- Calculate $D = H_3(pk_A,pk_B,pk_A^b)$, $d = H_3(X_A,pk_B,X_A^b)$.
- The following equations are calculated by Lagrangian interpolation according to $S = \{S_{x,i}\}_{i=1}^k, S_{x,i} = H_2(id_i,D)$, and finally the symmetric key $K = H_5((E' \cdot V')^d)$ is output:

$$\lambda_{i,j} = \prod_{j=1,j\neq i}^{k} \frac{S_{x,j}}{S_{x,j} - S_{x,i}} \tag{14}$$

$$E' = \prod_{i=1}^{k} (E_{1,i})^{\lambda_{i,j}} \tag{15}$$

$$U' = \prod_{i=1}^{k} (U_{1,i})^{\lambda_{i,j}} \tag{16}$$

$Decrypt(encM,K)$: The destination node can decrypt $encM$ according to the obtained symmetric key and finally get the message plaintext M.

3) SECURITY ANALYSIS. **Threat Model:** This section defines the threat model of the scenario through the behavior of the nodes involved in data transmission in the network, as shown in Fig. 4.

Source node: The source node in the WSN sends the collected data to the destination node, and we assume that the data sender is honest (i.e., the data is genuine). But, there is a possibility of attackers in the network impersonating the identity of the real data sender, who can encrypt real data and forge fake packet encryptions to contaminate the sensed data.

Destination node: The destination node in the WSN acts as the receiver of the stored and analyzed data. We assume that the data receiver is malicious so that destination nod can launch a conspiracy attack with a proxy node, thus bypassing the restrictions of heavy encryption and compromising the confidentiality of the data.

Proxy node: It is assumed that the proxy nodes are semi-trustworthy, and some of them may eavesdrop on the data content or perform dishonest encryption.

External attacker node: Attackers cannot access to data directly, but they can compromise from within or outside the network.

Security analysis: Based on the threat model presented, the data is encrypted at the source node, then forwarded to the proxy node, and finally received and decrypted by the destination node. There they attack some malicious at any point. They can falsify identity information or even damage the sensor node physically, which can lead to data leakage. With the adoption of the threshold-based proxy re-encryption scheme in this chapter, the problems posed by the threat model can be effectively avoided.

Identity forgery: The problem of identity forgery is a hidden problem caused by the source node in the threat model. Since the

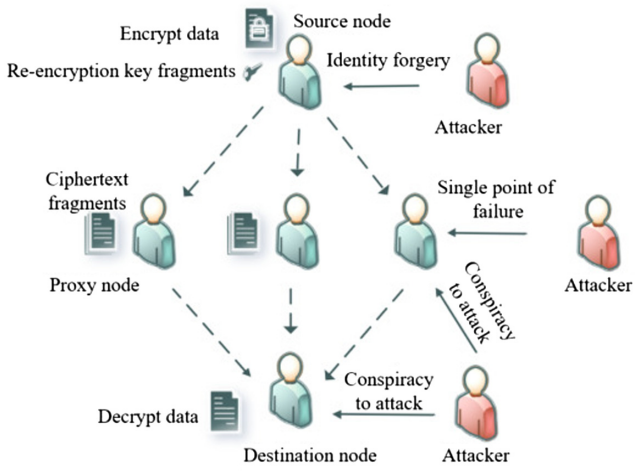

Fig. 4. Threat model.

public key encryption algorithm allows any node to encrypt the plaintext of a message with the public key of source node, it is possible for an attacker to forge an identity and impersonate the source node to encrypt the data. To prevent this, we uses a digital signature to verify the source node's identity to the data recipient. The digital signature (σ_1,σ_2) of the scheme is stored in a fragment of the re-encryption key $regen_frag$, and it cannot be sent directly to the destination node for verification. Therefore, we avoid the leakage of the identity of the source node due to monitoring. The destination node takes the digital signature as part of the shared data and cannot verify the signature until the ciphertext has been decrypted.

Conspiracy attacking: If the proxy node collude with a destination node, it will choose to leak the re-encryption key directly to the destination node who can decrypt the data at will without any constraints. Our method use a threshold-based proxy re-encryption scheme, in which the re-encryption key is constructed into multiple key fragments $regen_frag$, then distributed to multiple proxy nodes in the network. Such an approach disperses trust among multiple proxy nodes, and if destination node wants to launch a conspiracy attack, it needs to collude with at least the number of k proxy node, which is equivalent to solving the threshold secret sharing problem. As we know, it is computationally impossible, so our method increases the difficulty of the conspiracy attack greatly.

Single point of failure: Due to the WSN is in the middle of an open network, there are the possibility of sensor nodes being deployed in enemy territory. When a node is captured by an enemy, there is the potential for the node to be compromised. When a particular proxy node is attacked, it will disrupt the process of encrypting the network data transmission. Since our method uses a threshold-based proxy re-encryption scheme with multiple proxy nodes, the destination node only needs to obtain the number of k fragment of the key to decrypt. So it allows the data encryption process to remain intact even if some of the proxy nodes fail.

IV. SIMULATION SETUP AND EXPERIMENTAL RESULTS

This section describes the experimental evaluation of ACOTPRE. The simulation model, performance metrics, and comparative analysis are described in this section.

A. SIMULATION MODEL

The performance of the proposed scheme was tested using Network Simulator version 3.27. A total of 50 nodes were randomly distributed in an area of 1000 m × 1000 m, and the transmission distance was fixed at 100 m. The source node and the target node were randomly selected from the network. Table I shows the simulation configuration in experiments.

B. EXPERIMENTAL RESULTS

The PDR, EED, and ARE were used to evaluate the proposed scheme.

1) PERFORMANCE INDICATORS. *Packet delivery ratio (PDR)*: The efficiency of any routing algorithm can be analyzed by estimating the number of data packets communicated to sink node. So the PDR is the ratio of the number of successfully received data packets to the total number of data packets sent:

$$PDR = \frac{\sum N_r}{\sum N_s} \times 100\% \tag{17}$$

where N_r is the number of data packets successfully received by the target node and N_s is the total number of data packets sent by the source node. *End-to-end delay (EED)*: The EED represents the time taken by a data packet to travel from the source node to the destination node. The delay should be less to achieve effective routing:

$$\overline{EED} = \frac{\sum T_r(i) - T_s(i)}{nN} \tag{18}$$

where $T_r(i)$ is the time at which the destination node receives the data packet and $T_s(i)$ is the time at which the source node sends the data packet. The total number of nodes in the network is n, and nN is the total number of data messages. *Average Residual Energy (ARE)*: ARE is obtained by calculating the energy level consumed by each node at the end of the simulation (i.e., packet transmission). In a WSN, every data packet sent to the sink node consumes a certain amount of energy. The energy consumption of the network can be determined by calculating the ARE remaining in the network. The larger the ARE remaining in the network, the lesser the ARE consumed and the longer the life cycle of the network:

$$ARE = \frac{\sum_{i=1}^{n} E_i}{n} \tag{19}$$

where E_i is the total number of nodes in the network and n is the energy remaining in each node.

2) PERFORMANCE ANALYSIS. This section compares the ACOTPRE with other existing methods, namely the AODV

Table I. Simulation parameters.

Parameters	Value
Range of simulation	1000 m × 1000 m
Number of nodes	50
Transmitting power	24·75 mW
Receiving power	13·5 mW
Packet transmission rate	40 kbps
Packet size	100bit
Initial energy of the node	1 J
Range of node communication	100 m

protocol and Refine Trust Energy (ReTE)-AODV, in terms of PDR, EED, and ARE.

PDR: Fig. 5 depicts the variation in PDR with the number of nodes, considering the AODV, ReTE-AODV, and ACOTPRE. It can be found that as the number of nodes increases, the PDR gradually decreases. This result is due to the more the number of nodes, the higher the network congestion, causing more link failures. However, the PDR for ACOTPRE increases considerably as compared to both protocols. When the number of nodes is kept constant at same, the PDR of proposed scheme is approximately increased by 19% as that of ReTE-AODV. From the Fig. 5, it is clear that by increasing the node count, the gap of PDR between the ACOTPRE and AODV has gradually increased, from an increase of 22% to 124%.

EED: From Fig. 6, it is obvious that EED increases with increase in the number of nodes. We notice that ACOTPRE has lower delay than AODV, then the delay is reduced by 0·18 s on average. The reason is that the classic AODV algorithm does not use trust model, while ReTE-AODV and our method are both trust-based algorithms to improve performance by eliminating malicious and selfish nodes in routing and reducing end-to-end delay. Since nodes have limited memory, ACOTPRE requires larger computing requirements but saves some storage. Then the ACOTPRE showcases EED slightly higher than that of ReTE-AODV with better reliability. The average EED of the proposed scheme was found to be 0·998 s, whereas ReTE-AODV exhibited an average EED of 0·814 s.

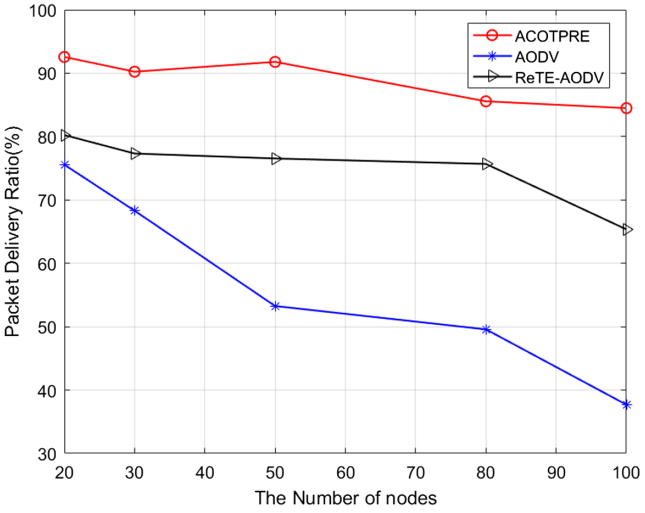

Fig. 5. Packet delivery ratio comparison with different nodes count.

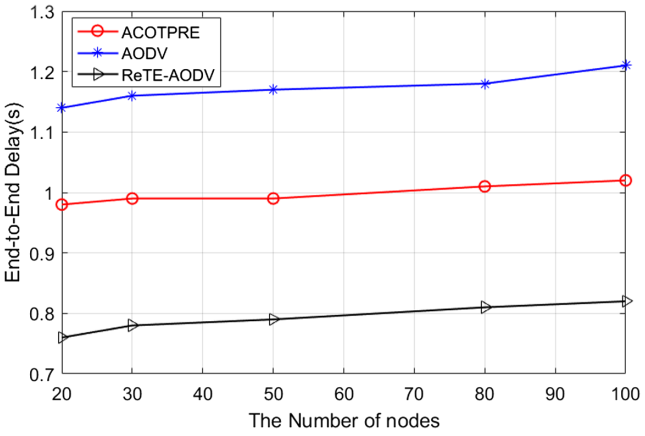

Fig. 6. End-to-end delay comparison with different nodes count.

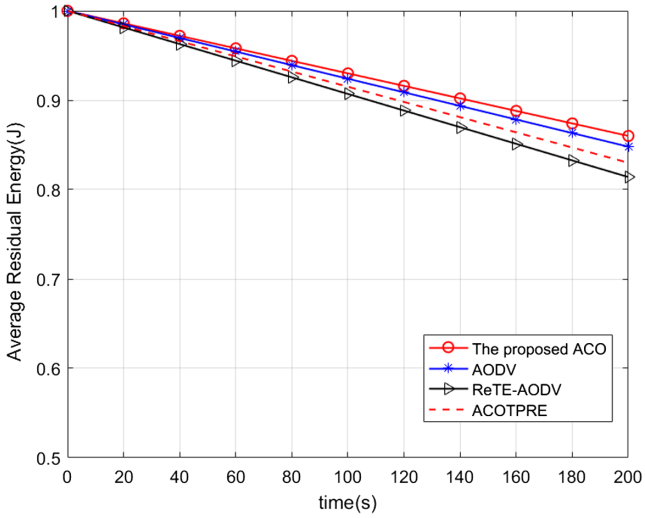

Fig. 7. Average energy remained comparison with different nodes count.

ARE: Fig. 7 shows the ARE change of nodes corresponding to the ACOTPRE, AODV, and ReTE-AODV for a fixed number of network nodes of 50, which also compares this paper's ACOTPRE scheme (i.e., without adding proxy re-encryption). The ACOTPRE consumes more energy than the AODV. However, ACOTPRE is more secure, and its high energy consumption does not affect the selection of transmission path. The average residual energy of ACOTPRE is higher than RETE-AODV, because when ants choose the optimal path, the pheromone concentration update strategy is based on the energy in the network so that it can balance the energy consumption of the network. Although the ACOTPRE contains proxy re-encryption based on threshold secret sharing, which requires the source and destination nodes to compute polynomial interpolation, the other proxy nodes only perform two exponential operations, so the overall computational energy consumption of the network is not significantly increased.

C. SYSTEM SECURITY

This paper proposes the deployment of an AOCTPRE security strategy in the data transmission path selection phase and data encryption phase. By establishing a trust assessment model between nodes in the path selection phase, the number and content of data packets are identified as direct trust indicators. WSNs can defend against most attacks from internal attacker nodes effectively that incorporate a trust mechanism. This security mechanism is a passive defense mechanism, which cannot identify and remove external attackers disguised as normal nodes. And its defense capability has certain limitations. Therefore, in the data encryption phase, a threshold-based proxy re-encryption scheme is constructed to build a defense system that organically combines active defense and passive defense, so as to achieve security protection for the whole network.

V. CONCLUSION

In this paper, we proposed a data transmission mechanism in WSN that enforces both security and performance. The proposed mechanism is based on the ACO during a path selection phase and the threshold PRE during a data encryption phase. ACOTPRE solves the data transmission path problem by constructing a new pheromone factor that includes trust, energy, and signal strength. A threshold proxy re-encryption method is used to solve security issues related to data encryption. The security of our scheme relies on the concept of the trust model and threshold secret sharing to resist internal attacks and external attacks. We have confirmed the validity and performance of our model via simulation studies. In our future work, we plan to conduct a more in-depth examination about computational complexity and network delay.

ACKNOWLEDGMENTS

This work was supported in part by Beijing Municipal Natural Science Foundation (19L2020), National Key Research and Development Project (Key Technologies and Applications of Security and Trusted Industrial Control System NO.2020YFB2009500).

References

[1] F. Meneghello et al., "IOT: internet of threats? A survey of practical security vulnerabilities in real iot devices," IEEE Internet Things J., vol. 6, no. 5, pp. 8182–8201, 2019.

[2] Y. Chen, Service-Oriented Computing and System Integration: Software, IoT, Big Data, and AI as Services, 7th edition, State of Iowa, U.S.A.: Kendall Hunt Publishing, 2020.

[3] Juniper Research. Accessed Nov. 2020. [Online]. Available: https://www.juniperresearch.com/document-library/white-papers/industrial-revolution-4-the-future-of-iiot.

[4] Huang K et al., "Multilinear plus sparse based tensor completion for long-term operating large-scale and heterogeneous sensor networks," IEEE Trans. Wireless Commun., vol. 19, no. 10, pp. 6301–6315, 2020.

[5] V. B. Reddy, A. Negi, and S. Venkataraman, "Communication and data trust for wireless sensor networks using d–s theory," IEEE Sens. J., vol. 17, no. 12, pp. 3921–3929, 2017.

[6] L. Zhong, R. Wan, and X. Si, "An improved aco-based security routing protocol for wireless sensor networks," In Proc. Conf. Comput. Sci. Appl., Wuhan, China, pp. 90–93, 2013.

[7] S. Hemalatha and V. Rajamani, "VMIS: an improved security mechanism for WSN applications," in Int. Conf. Sci. Eng. Manag. Res. (ICSEMR), Chennai, India, pp. 1–3, 2015.

[8] B. Ayyappan and P. M. Kumar, "Security protocols in WSN: a survey," in Proc. 3rd Int. Conf. Sci. Technol. Eng. Manag. (ICONSTEM), Chennai, India, pp. 301–304, 2017.

[9] C. Iwendi, Z. Zhang, and X. Du, "Aco based key management routing mechanism for WSN security and data collection," in Proc. 2018 IEEE Int. Conf. Ind. Technol. (ICIT), Lyon, France, pp. 1935–1939, 2018.

[10] B. Patil and R. Kadam "A novel approach to secure routing protocols in WSN," in Proc. 2nd Int. Conf. Inven. Syst. Control (ICISC), Coimbatore, India, pp. 1094–1097, 2018.

[11] P. Sethuraman and N. Kannan "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET," Wireless Netw., vol. 23, no. 7, pp. 2227–2237, 2017.

[12] G. Hatzivasilis, I. Papaefstathiou, C. Manifavas, "Scotres: secure routing for IOT and CPS," IEEE Internet Things J., vol. 4, no. 6, pp. 2129–2141, 2017.

[13] A. A. Pirzada, A. Datta, and C. Mcdonald, "Propagating trust in ad-hoc networks for reliable routing," in International Workshop on Wireless Ad-hoc Networks, Oulu, Finland: IEEE, 2004, pp. 58–62.

[14] S. Karthick, E. S. Devi, and R. V. Nagarajan, "Trust-distrust protocol for the secure routing in wireless sensor networks," in Proc. Int. Conf. Algorithms, Methodol. Models Appl. Emerging Technol. (ICAMMAET), Chennai, India, pp. 1–5, 2017.

[15] N. Djedjig et al., "Trust-aware and cooperative routing protocol for IOT security," J. Inf. Secur. Appl., vol. 52, p. 102467, 2020.

[16] X. Zhou and B. Qin, "Secure routing algorithm based on energy optimization for wireless sensor networks," Acta Electron. Sin., vol. 35, no. 1, pp. 54–57, 2007.

[17] W. Li et al., "An identity-based secure routing protocol in WSNS," in Proc. 7th ICCIS, Hainan, China, pp. 703–706, 2011.

[18] R. Sreevidya and G. Nagaraja, "Secure multicast routing for wireless sensor networks using aco-aodv with dhke cryptosystem," In Proc. ICCMC, Erode, India, pp. 733–737, 2018.

[19] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. ICTACT, Espoo, Finland, vol. 1403, pp. 127–144, 1998.

[20] G. Ateniese et al., "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM TISSEC, vol. 9, no. 1, pp. 1–30, 2006.

[21] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. 5th ICACNS, Heidelberg, Germany, pp. 288–306, 2007.

[22] S. Lou and Z. Cao "Identity-based proxy re-encryption with threshold multi-proxy," J. Nat. Sci. Heilongjiang Univ., vol. 27, no. 2, pp. 151–156, 2010.

[23] C. Xi et al., "Threshold proxy re-encryption and its application in blockchain," in Proc. ICCCS, Haikou, China, pp. 16–25, 2018.

[24] C. Ge et al., "A source hiding identity-based proxy reencryption scheme for wireless sensor network," Secur. Commun. Netw., vol. 2018, pp. 1–8, 2018.

[25] K. Liang et al., "A conditional proxy broadcast re-encryption scheme supporting timed-release," in Proc. ISPEC, Lanzhou, China, pp. 132–146, 2013.

[26] M. Kambombo, P. Anand, and R. Seungmin, "Time-and-id-based proxy reencryption scheme," J. Appl. Math., vol. 2014, pp. 1–7, 2014.

[27] Fan C et al., "Provably secure timed-release proxy conditional reencryption," IEEE Syst. J., vol. PP, no. 4, pp. 1–12, 2017.

[28] B. Muthusenthil, D. Nivetha, and H. Kim, "Reencryption scheme for secure data sharing," in Proc. ICCSP, Melmaruvathur, India, pp. 1170–1174, 2016.

[29] S. Kanchan and N. Chaudhari, "Integrating group signature scheme with non-transitive proxy re-encryption in vanet," in Proc. ICCAST, Pune, India, pp. 227–231, 2016.

[30] J. Li, C. Ma, and Q. Zhao, "Resplittable threshold multi-broker proxy re-encryptionscheme from lattices," J. Commun., vol. 38, no. 5, pp. 157–164, 2017.

[31] Y. Zhu and G. Dou, "A WSN security data fusion method based on multidimensional trust," J. Wuhan Univ., vol. 59, no. 2, pp. 193–197, 2013.