Received February 8, 2020, accepted March 7, 2020, date of publication March 16, 2020, date of current version March 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2981115

Joint Energy-Saving Scheduling and Secure Routing for Critical Event Reporting in Wireless Sensor Networks

WEI FENG[1,2,3], FENG WANG[1], DAN XU[1], YINGBIAO YAO[1], XIAORONG XU[1], (Member, IEEE), XIANYANG JIANG[1], AND MINGXIONG ZHAO[4]

[1]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
[2]College of Telecommunication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[3]Sunwave Communications Company Ltd., Hangzhou 310051, China
[4]School of Software, Yunnan University, Kunming 650091, China

Corresponding authors: Yingbiao Yao (yaoyb@hdu.edu.cn) and Mingxiong Zhao (mx_zhao@ynu.edu.cn)

This work was supported in part by the Public Welfare Plan Project of Zhejiang Province under Grant LGG19F020014, in part by the Natural Science Foundation of Zhejiang Province under Grant LY19F010011, in part by the National Natural Science Foundation of China under Grant 61801418, in part by the Yunnan Applied Basic Research Project under Grant 2019FD-12, and in part by the Open Foundation of Key Laboratory in Software Engineering of Yunnan Province under Grant 2017SE203.

ABSTRACT With the growing concerns about energy saving and security problems in wireless sensor networks (WSNs), we investigated a joint energy saving scheduling and secure routing algorithm for critical event reporting in WSN. When a critical event has been detected, the notification must be safely sent to the sink node through the uplink transmission, and the sink node needs to broadcast the alarm messages to the whole network through the downlink transmission. In the uplink, a joint power allocation and secure routing strategy (JPASR) has been proposed to maximize the routing secure connection probability (RSCP) under the constraint of power. Meanwhile, combined with the level-by-level sleeping scheduling method, the energy-saving and secure uplink transmission can be guaranteed. In the downlink, an energy-first multi-point relays set selection mechanism (EFMSS) is designed to choose the backbone nodes to broadcast messages, and the backbone nodes are waken up by the same level-by-level sleeping scheduling method as the uplink transmission. With the two-step procedure, the critical events are appropriately dealt with and the responses are broadcast to the whole network. Extensive simulations results demonstrate that the energy saving and security performances of the proposed method are superior to the existing ones.

INDEX TERMS Secure routing, energy saving, sleeping scheduling, critical event reporting, wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks (WSNs) have grown rapidly in the recent years and are widely applied to communication, surveillance, health care and disaster management system and so on [1], [2]. Sensor nodes transmit, receive, route and sense information from/to its neighbors or base stations, which induces largely energy consumption. However, most of sensor equipments mainly depend on battery or micro motor power supply, which makes energy invaluable for WSNs. To realize energy saving in WSNs, many scholars have studied and put forward effective solutions in order to realize energy saving in sensor networks wherein they focused on the following three areas: (1) optimization technology based on link restoration [3]–[5]; (2) load balancing and energy saving optimization [6]–[10]; (3) energy optimization technology based on distance [11]–[16].

To be specific, a range-based opportunistic routing protocol (ROR) was proposed in [3] to minimize energy consumption by selecting the forwarding list. In [4], a multi-hop graph-based approach for an energy-efficient routing (MH-GEER) protocol extended the networks' life spans by exploring the energy levels in the entire network and using the energy levels to select the next hop in a probabilistic, intelligent way. In [5], a check point route recovery algorithm (CPRAA) was presented. The algorithm could autonomously maintain a subset of the actor nodes in accordance with the node energy level to keep network connectivity.

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

The network lifetime was prolonged in [6] by reconstructing the network to regain energy balance as soon as the energy consumption of some nodes exceeded a given energy threshold. In [7], the non-uniform sampling and reliable routing were jointly designed to save the energy. In [8], a distributed load-balancing clustering algorithm was presented to improve network life cycle. In [9], a Cost and Payment-based clustering Algorithm (CoPA) was proposed for achieving energy efficiency in WSNs, and CoPA produced a balanced distribution of responsibilities and energy consumption between the sensor nodes. In [10], an evolutionary routing anti-coordination game was established to balance the energy consumption of the sensor nodes by reducing congestion and optimally distributing data traffic among multiple heterogeneous paths. In [11], a cluster-based protocol called power efficient and adaptive latency was proposed to extend the network lifetime and introduced an acceptable transmission latency. The cluster heads was elected according to the desired percentage of cluster heads, current round, the distance between sensor nodes and their nearest base station and remaining energy. An optimal-distance-based transmission strategy was put forward in [12] to minimize the energy consumption of sensor nodes with maximal energy consumption throughout the network. In [13], an energy efficient data routing for in-network aggregation (EEDRINA) was exploited to aggregate redundant data at transitional node for critical event monitoring in WSNs. The method, which reduced the size and the number of exchanged messages, and thus, energy was saved. In [14], a general self-organized tree-based energy-balance routing protocol (GSTEB) was proposed, which built the routing tree based on both energy consumption and energy balancing. Different from the aforementioned methods, ECQSR in [15] chose the next neighbor node based on both the maximization of network lifetime and the balance of energy consumption across multiple nodes by using the concept of service differentiation. In [16], a traditional flow augmentation (FA) routing algorithm was designed to choose the route that can maximize the network lifetime. The routing metric was formulated based on node transmission power as well as residual node energy, since a good candidate node should consume less power and has high residual energy.

The optimization schemes in [3]–[16] can effectively reduce energy consumption and prolong network lifetime. However, the security problem that may exist in WSNs has been ignored. In fact, WSNs have faced series of security problems, such as information stealing and modification, DOS attacks and so on [17], [18]. These problems disturb the normal information transmission, and even lead to the disclosure of confidential information. Especially in recent years, WSNs are increasingly applied to transmit privacy information, such as human health information and home video monitoring information, where information leakage violates human rights and causes serious consequences. Thus, it is particularly important to realize information security transmission in WSNs. In the literatures, most of the researches on the security of sensor networks focused on the upper layer of OSI model. For example, to prevent WSNs from eavesdropping, cryptographic technology was utilized in [17]; To guard against traffic analysis attacks, packet transmission rate was controlled in [18]. However, these solutions based on the upper layers will bring a large amount of running and storage overhead, which is not adaptable to WSNs due to the energy, memory and other limitations on sensor nodes.

Recently, physical layer security has emerged as a complementary technology to the upper-layer-based method, which can defend against eavesdroppers by exploiting the physical characteristics of wireless channels [19]–[22]. The authors in [19] applied the physical layer security technology and proposed a lightweight and privacy-preserving mutual user authentication protocol in which only the user with a trusted device had the right to access the industrial WSNs. In [20], a physical layer (PHY) authentication technique for wireless implantable medical devices was presented. The authors in [21] developed a framework for exploiting the potential benefits of physical layer security in three-tier WSNs using stochastic geometry and multiple-antenna technique. The above mentioned methods [19]–[21] all adopted physical layer security technology, but ignored considering energy limitations in WSNs. The authors in [22] investigated destination assisted cooperative jamming (DACJ) for physical layer security and physical layer network coding (PNC) in two-hop WSNs. The proposed two-phase algorithm optimized the power allocation in WSNs, however, it could just be applied in the two-hop network with one source and one destination only and was lack of universality.

Therefore, a handful of researches have investigated that research on energy efficient physical layer security technology in WSNs, and it is still an intractable problem. The authors in [23] investigated the scene where there is one sink, multiple legitimate nodes and position-unknown eavesdroppers. When an emergency have occurred, the nodes in WSN needed to safely route the event or alarm to the sink node through the uplink transmission and the sink node processed the information and broadcast the notification or warning to the whole network through the downlink transmission.

Different from the previous researches, we develops a tractable framework that jointly considers energy-saving secure routing in the uplink and energy-saving sleeping scheduling in uplink and downlink for event supervisory control in WSNs. The contributions are given as follows:

1) In the uplink transmission, a joint power allocation and secure routing scheme (JPASR) is proposed. In JPASR, a power minimization problem is modeled under the constraints of end-to-end bit error ratio (BER) and the routing strategy that can maximize the routing secure connection probability (RSCP) with the existence of multiple position-unknown eavesdroppers. After a series of solution procedures, the secure routing can be computed using the classical Dijkstra's algorithm, and the transmission power along the secure routing is allocated according to the power allocation

stategy. JPASR not only ensures the information transmission security but also reduces power consumption.

2) In the downlink transmission, an energy first multi-hop relays set selection strategy (EFMSS) is proposed to choose one-hop neighbors with more residual energy as multi-hop relays (MPRs) to route messages from the sink node to the whole network in the broadcasting procedure. Only the MPRs need to retransmit the packet from their neighbors, and the use of MPR set reduces the retransmitted message number. EFMSS balances energy consumption and prolongs the network lifetime.

3) Throughout the uplink and downlink transmission, a hierarchical sleeping scheduling strategy is designed to save the energy consumption, which is easier to complement than the previous level-by-level offset [24]. The layers are defined by the hop number away from the sink node, which is generated according to different routing algorithms in the uplink and downlink, respectively. In the uplink, the secure routing algorithm is applied to find the hop number to the sink node. In the downlink, the shortest routing algorithm during the MPR's selection procedure decides the layer architecture. The sleeping scheduling strategy based on the predefined layer is designed to save energy further.

The rest of this paper is given as follows. In Section II, we describe the system model and related concepts. In Section III, JPASR is proposed for the uplink transmission. In Section IV, the energy efficient sleeping scheduling method is presented for the downlink communication. The simulation is presented in Section V. Section VI gives our conclusion and future directions.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. SYSTEM MODEL

Consider a WSN with N legitimate nodes and M independent eavesdroppers $E_j, j \epsilon \{1, 2, 3, \ldots, M\}$. Both legitimate nodes' and eavesdroppers' positions are subject to Poisson distribution with density λ_L and λ_E, respectively, where the legitimate nodes' locations are available and the eavesdroppers are passive. Both channel state information (CSI) and the location are unknown to the legitimate nodes. Each node equips with an omni-directional antenna and works in time-division multiplexing (TDM) mode. Relay nodes use decode-and-forward (DF) mode to transmit data.

The proposed scheme can be realized according to the following two stages:

- Phase 1: During the $(2k-1)$-th duty cycle, any node who has detected emergency event uses the shortest path selected by JPASR to send the alarm message to the sink node. Every node along the route is waken up according to the sleeping scheduling strategy and then forwards the alarm message with the transmission power allocated by JPASR. The first stage is described in Fig. 1.
- Phase 2: During the $2k$-th duty cycle, the sink node forwards the control message to the whole network through the MPR set, which is chosen by EFMSS. During the broadcasting process, nodes are waken up in the layer-by-layer pattern. The second stage is shown in Fig. 2.

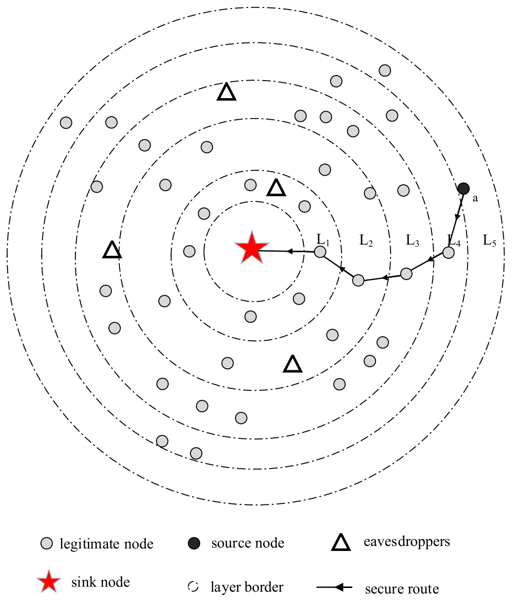


FIGURE 1. Uplink: event detection and report in the $(2k-1)$-th duty cycle.

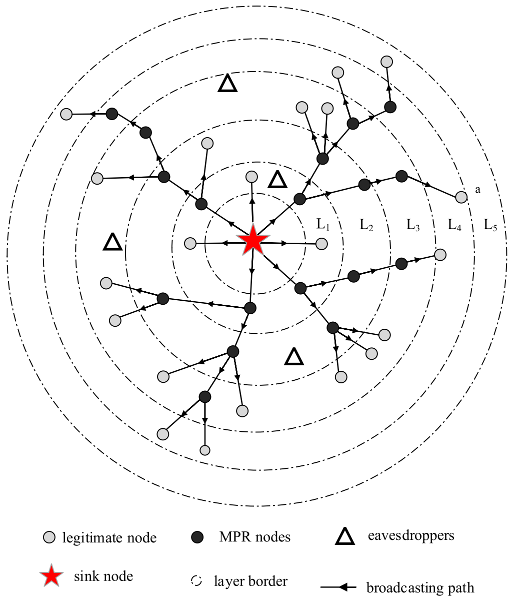


FIGURE 2. Downlink: notification broadcast in the $2k$-th duty cycle.

B. RELATED CONCEPTS

1) RSCP

When the message is transmitted from node A_i to node A_{i+1}, the received signal noise ratio (SNR) at node A_{i+1} and eavesdropper E_j can be described as

$$\sigma_{A_iA_{i+1}} = \frac{P_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}, \tag{1}$$

$$\sigma_{A_iE_j} = \frac{P_{A_i}\left|h_{A_iE_j}\right|^2}{d^{\alpha}_{A_iE_j}}, \tag{2}$$

where P_{A_i} represents the transmission power of legitimate node A_i, $h_{A_iA_{i+1}}$ and $d_{A_iA_{i+1}}$ represent the channel fading coefficient and the distance between node A_i and node A_{i+1} respectively, $h_{A_iE_j}$ and $d_{A_iE_j}$ represents the channel fading coefficient and the distance between node A_i and eavesdropper E_j, respectively, and α represents path loss factor. In this paper, $\left|h_{A_iA_{i+1}}\right|^2$ and $\left|h_{A_iE_j}\right|^2$ are assumed to follow an independent exponential distribution with unit mean.

Consider an R-hop route $L =< A_1, A_2, \ldots, A_{R+1} >$. RSCP Pr in the non-collusion case can be expressed as [23]

$$\begin{aligned}\Pr &= \Pr\Big[\log_2\left(1+\min_{i=1,\ldots,R}\sigma_{A_iA_{i+1}}\right)\\&\quad-\log_2\left(1+\max_{E_j\epsilon M}\left\{\sum_{i=1}^{R}\sigma_{A_iE_j}\right\}\right)>0\Big]\\&\approx\exp\left[-K\left(\sum_{k=1}^{R}P_{A_k}\sum_{i=1}^{R}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}}\right)^{\frac{\alpha}{2}}\right]\end{aligned}\tag{3}$$

where $K = \pi\lambda_E\Gamma(1+\dfrac{2}{\alpha})\Gamma(1-\dfrac{2}{\alpha})$, $\Gamma(\cdot)$ is a gamma function, λ_E is the density of the eavesdroppers, and P_{A_i} represents the transmission power of legitimate node A_i.

2) END-TO-END BER

Since $|h|^2$ is an exponential distribution with unit mean value, the SNR σ is also an exponentially distributed random variable. The cumulative distribution function (CDF) of σ can be expressed as follows

$$F_{\sigma_i} = 1 - e^{-\sigma\sqrt{\sigma_i}},\tag{4}$$

where $\bar{\sigma}_i = P_{A_i}/d^{\alpha}_{A_iA_{i+1}}$ is the average SNR of the ith hop.

In [25, Ch.5], the single-hop instantaneous BER $\zeta_i(\sigma)$ for any coding scheme can be expressed as

$$\zeta_i(\sigma) = aQ(\sqrt{b\sigma}),\tag{5}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_0^{+\infty} e^{-u^2/2}du$, (a, b) is the constant determined by the modulation method.

It is also shown in [26] that the instantaneous BER $\zeta_i(\sigma)$ and the average BER $\bar{\zeta}_i(\sigma)$ meet the following relationship:

$$\bar{\zeta}_i(\sigma) = -\int_0^{+\infty}\zeta_i^{'}(\sigma)F_{\sigma_i}(\sigma)d\sigma,\tag{6}$$

where $\zeta_i^{'}(\sigma)$ denotes the derivation of the instantaneous BER.

Therefore, the average BER $\bar{\zeta}_i(\sigma)$ can be obtained as

$$\bar{\zeta}_i(\sigma) = \frac{a}{2}\sqrt{\frac{b}{2\pi}}\int_0^{+\infty}\frac{e^{-\frac{b\sigma}{a}}}{\sqrt{\sigma}}F_{\sigma_i}(\sigma)d\sigma.\tag{7}$$

Substituting equation (4) into the upper formula, the average BER $\bar{\zeta}_i(\sigma)$ can be proved to meet the following inequation

$$\begin{aligned}\bar{\zeta}_i(\sigma) &= \frac{a}{2}-\frac{a}{2}\frac{\sqrt{(b\bar{\sigma}_i)^2+2b\bar{\sigma}_i}}{b\bar{\sigma}_i+2}\leq\frac{a}{2}-\frac{a}{2}\frac{\sqrt{(b\bar{\sigma}_i)^2+2b\bar{\sigma}_i+1}}{b\bar{\sigma}_i+2}\\&=\frac{a}{2}-\frac{a}{2}\frac{\sqrt{((b\bar{\sigma}_i+1)^2}}{b\bar{\sigma}_i+2}=\frac{a}{2}-\frac{a}{2}\cdot\frac{((b\bar{\sigma}_i+1)}{b\bar{\sigma}_i+2}\\&=\frac{a}{2\,(b\bar{\sigma}_i+2)}\approx\frac{a}{2b\bar{\sigma}_i}=\frac{a}{2b}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}}.\end{aligned}\tag{8}$$

The relationship between the average BER of the ith hop and the end-to-end average BER is given as [27]

$$\bar{\zeta}_L = \sum_{i=1}^{R}\left(\bar{\zeta}_i\prod_{j=i+1}^{R}(1-2\bar{\zeta}_j)\right)\approx\sum_{i=1}^{R}\bar{\zeta}_i.\tag{9}$$

Combine equation (8) with (9), we can obtain $\bar{\zeta}_L = \frac{a}{2b}\sum_{i=1}^{R}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}}$.

Define $\bar{\zeta}_L$ threshold as ζ_{TH}, the system BER constraint condition can be denoted by

$$\frac{a}{2b}\sum_{i=1}^{R}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}}\leq\zeta_{\mathrm{TH}}.\tag{10}$$

3) HIERARCHICAL SLEEPING SCHEDULING STRATEGY

Due to the TDM model, we divide the time into uniform slots equal to the frame transmission time, and assume that the channel is quasi-static i.e., during one timeslot the channel is stable and central clock is needed to synchronize all nodes. Successive T timeslots comprise a duty cycle. As shown in Fig. 3, the odd duty cycle $(2k-1)$ is allocated to the uplink transmission, where $k = 1, 2, \cdots$. The even duty cycle $(2k)$ is for the downlink transmission. In each duty cycle, nodes wake up periodically according to their layers generated by different routing algorithms for the uplink and downlink transmission, respectively. It induces that the same node is likely to be partitioned into different layers in the uplink and downlink transmission, respectively, such as node a in Fig. 1 and Fig. 2. Define the same timeslot number T for the uplink and downlink transmission, i.e., $T = \max\{h_{\mathrm{up}}, h_{\mathrm{down}}\}$, where h_{up} and h_{down} are the maximal layer numbers in the uplink and downlink, respectively. To simplify discussion, we assume that the maximal layer numbers h_{up} and h_{down} are the same for both uplink and downlink without impacting on the sleeping scheduling strategy. As shown in Fig. 1 and Fig. 2, nodes are divided into different layers labeled by $L_1, L_2, \ldots, L_T$ based on their hop numbers away from the sink node and waken up in different timeslots depending on the corresponding duty cycle.

III. UPLINK TRANSMISSION PROCEDURE

A. JPASR

Taking RSCP and end-to-end average BER into consideration, the uplink transmission optimization problem can be

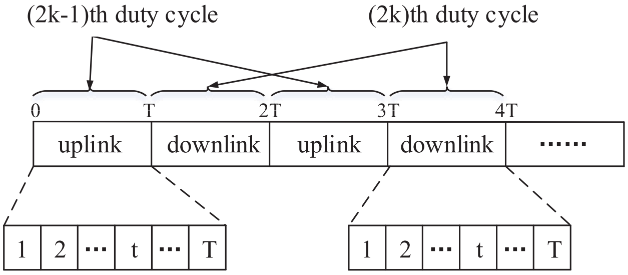


FIGURE 3. Duty cycle allocation.

modeled as

$$\min_{\varphi,P} \sum_{i=1}^{R} P_{A_i} \tag{11}$$

$$\text{s.t. } \frac{a}{2b}\sum_{i=1}^{R}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}} \leq \zeta_{\mathrm{TH}}, \tag{11a}$$

$$P_{A_i} \geq 0 \text{ for } i = 1, 2, \cdots, R, \tag{11b}$$

$$\varphi\left(A_i, P_{A_i}\right) = \arg \max_{L\epsilon L_{A_SA_D}} \exp\left[-K\left(\sum_{k=1}^{R}P_{A_k}\sum_{i=1}^{R}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}}\right)^{\frac{\alpha}{2}}\right], \tag{11c}$$

where $L_{A_SA_D}$ represents the route set from the source node A_S to the destination node A_D, and $\varphi\left(A_i, P_{A_i}\right)$ represents the chosen route with the maximum RSCP Pr defined in (3). To solve the optimization problem, we need to find the route which can maximize RSCP shown in constraint (11c).

Constraint (11c) can be transformed into the following problem

$$\max_{L\epsilon L_{A_SA_D}} \exp\left[-K\left(\sum_{k=1}^{R}P_{A_k}\sum_{i=1}^{R}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}}\right)^{\frac{\alpha}{2}}\right]. \tag{12}$$

Because both K and α are non-negative, (12) can be further written as

$$\min_{L\epsilon L_{A_SA_D}} \varphi\left(P\right)$$

$$\varphi\left(P\right) = \sum_{k=1}^{R}P_{A_k}\sum_{i=1}^{R}\frac{d^{\alpha}_{A_iA_{i+1}}}{P_{A_i}}, \tag{13}$$

where $\varphi\left(P\right)$ can be decomposed as

$$\varphi\left(P\right) = \sum_{i\epsilon L} d^{\alpha}_{A_iA_{i+1}} + \sum_{i,j\epsilon L, i<j}\left(\frac{P_{A_i}}{P_{A_j}}d^{\alpha}_{A_jA_{j+1}} + \frac{P_{A_j}}{P_{A_i}}d^{\alpha}_{A_iA_{i+1}}\right). \tag{14}$$

Applying the basic inequality $a + b \geqslant 2\sqrt{ab}(a > 0, b > 0)$, we can obtain

$$\varphi\left(P\right) \geq \sum_{i\epsilon L} d^{\alpha}_{A_iA_{i+1}} + \sum_{i,j\epsilon L, i<j} 2\sqrt{d^{\alpha}_{A_iA_{i+1}}d^{\alpha}_{A_jA_{j+1}}}$$
$$= \left(\sum_{i\epsilon L}\sqrt{d^{\alpha}_{A_iA_{i+1}}}\right)^2. \tag{15}$$

The condition holds if

$$\frac{P_{A_i}}{P_{A_j}}d^{\alpha}_{A_jA_{j+1}} = \frac{P_{A_j}}{P_{A_i}}d^{\alpha}_{A_iA_{i+1}}, \quad \text{for } i < j \text{ and } i, j\epsilon L. \tag{16}$$

With some mathematic manipulations, the power allocation condition for the transmission node on the given path L can be obtained as

$$P_{A_j} = P_{A_1}\sqrt{\frac{d^{\alpha}_{A_jA_{j+1}}}{d^{\alpha}_{A_1A_2}}}, \quad \text{for } j\epsilon L, \tag{17}$$

which means that maximum RSCP can be achieved ONLY when the nodes along the selected path transmit the messages with the obtained transmission power according to the above equation.

Substituting (17) into (11), we can reformulate (11) as

$$\min_{\varphi,P} \sum_{i=1}^{R} P_{A_i} \tag{18}$$

s.t. (11a), (11b),

$$P_{A_i} = P_{A_1}\sqrt{\frac{d^{\alpha}_{A_iA_{i+1}}}{d^{\alpha}_{A_1A_2}}} \quad \text{for } i = 1, 2, \cdots, R. \tag{18a}$$

Continue to substitute (18a) into (11a), we have

$$P_{A_1} \geq \frac{a}{2b}\frac{\sqrt{d^{\alpha}_{A_1A_2}}\sum_{i=1}^{R}\sqrt{d^{\alpha}_{A_iA_{i+1}}}}{\zeta_{\mathrm{TH}}}. \tag{19}$$

Combine (18a) and (18), then we get

$$\min_{P}\sum_{i=1}^{R}P_{A_i} = \min_{P}\left[P_{A_1}\cdot\left(1 + \sqrt{\frac{d^{\alpha}_{A_2A_3}}{d^{\alpha}_{A_1A_2}}} + \sqrt{\frac{d^{\alpha}_{A_3A_4}}{d^{\alpha}_{A_1A_2}}} + \cdots + \sqrt{\frac{d^{\alpha}_{A_RA_{R+1}}}{d^{\alpha}_{A_1A_2}}}\right)\right] \tag{20}$$

As shown in (20), for given route, to minimize the total power is to find the minimum value of P_{A_1}. Combining (19) with (20), the optimal power allocation for the source node A_1 on the given route can be obtained as

$$P^{*}_{A_1} = \frac{a}{2b}\frac{\sqrt{d^{\alpha}_{A_1A_2}}\sum_{i=1}^{R}\sqrt{d^{\alpha}_{A_iA_{i+1}}}}{\zeta_{\mathrm{TH}}}. \tag{21}$$

Substituting (21) into (18a), the optimal transmission power for node j on the given route can be achieved as

$$P^{*}_{A_j} = \frac{a}{2b}\frac{\sqrt{d^{\alpha}_{A_jA_{j+1}}}\sum_{i=1}^{R}\sqrt{d^{\alpha}_{A_iA_{i+1}}}}{\zeta_{\mathrm{TH}}}. \tag{22}$$

According to (11), we further get

$$\min_{L\epsilon L_{A_S A_D}} \sum_{i\epsilon N} \sqrt{d^{\alpha}_{A_iA_{i+1}}}. \tag{23}$$

For a WSN, the minimization problem (23) can be described as a a minimum weight routing problem in a known topology in which the routing metric is the node distance $\sqrt{d^{\alpha}_{A_jA_{j+1}}}$. This kind of method can be categorized into the classical least cost routing algorithm and can be solved by the Dijkstra's algorithm. The routing weight function is

$$w(d) = \sqrt{d^{\alpha}_{A_jA_{j+1}}}. \tag{24}$$

Resorting to (22), the total power consumption on the chosen routing L is

$$\sum_{i=1}^{R} P^{*}_{A_i} = \frac{a}{2b}\frac{\left(\sum_{i=1}^{R}\sqrt{d^{\alpha}_{A_iA_{i+1}}}\right)^2}{\zeta_{\text{TH}}}. \tag{25}$$

Finally, RSCP Pr in (3) can be computed according to

$$\text{Pr} = \exp\left[-K\left(\sum_{i=1}^{R}\sqrt{d^{\alpha}_{A_iA_{i+1}}}\right)^{\frac{4}{\alpha}}\right]. \tag{26}$$

Until now, we can find the secure route to transmit the secret information to the sink node and allocate the suitable transmission power to the nodes along the route. In order to ensure the route with no cycle and consistency, it is necessary to check the isotonicity and monotonicity [28] of the path weight function. Since the weights $\sqrt{d^{\alpha}_{A_jA_{j+1}}}$ are fixed positive and irrelevant, so it is easy to prove that the path weight function is strictly monotone and isotonic. Therefore, classical link state routing protocol can use Dijkstra's algorithm to achieve the route, such as Optimized Link State Routing (OLSR).

B. UPLINK SLEEPING SCHEDULING STRATEGY

According to the routing table generated by JPASR, each node knows both the maximal hop number T to sink node in the network and the hop number t from itself to the sink node. Resorting to the maximal hop number T, shown in Fig. 4, the network is divided into T layers, where each node belongs to the layer that is equal to the hop number t. In the layered architecture, the sink node acts as the core, and nodes with the same hop number constitute the node set for each layer. The details of scheduling strategy are further described in Fig. Fig. 4, where odd duty cycles are allocated to the uplink transmission. During the odd duty cycles, nodes in the t-th layer periodically wakes up in the $(T-t)$-th timeslot to receive data and $(T-t+1)$-th timeslot to transmit data, otherwise, they are in sleep mode.

C. IMPLEMENTATION OF UPLINK TRANSMISSION

The implementation steps of uplink transmission are shown as follows:

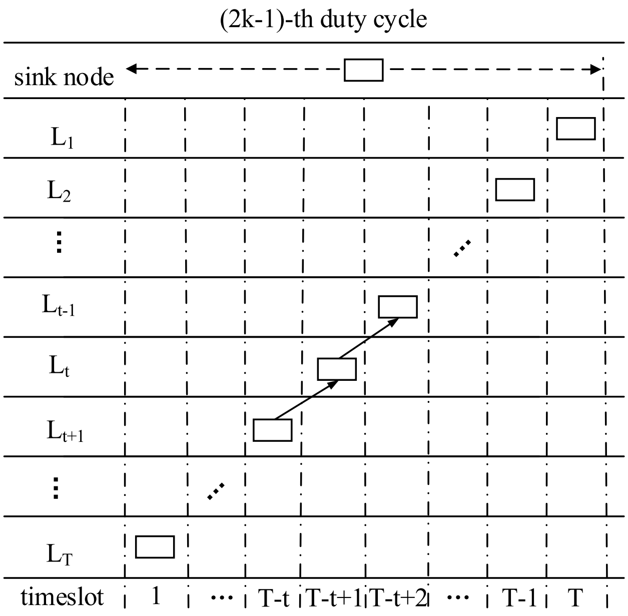


FIGURE 4. Hierarchical sleeping scheduling strategy for the uplink transmission.

1) The network with N legitimate nodes and M eavesdroppers is generated according to the Poisson distribution, BER threshold ζ_{TH} is defined and the distance d is broadcast to the whole network in the initialization stage.
2) Routing: each legitimate node takes $\sqrt{d^{\alpha}_{A_iA_{i+1}}}$ as link weight, uses Dijkstra's algorithm to calculate route to the sink node and updates routing table.
3) Power allocation: each transmission node along the route calculates the transmission power according to formula (22).
4) Uplink Scheduling: according to the routing table generated in Step 2), each node knows the maximal hop number T and the hop number t from itself to the sink node. All nodes, t-hop far away from the sink node, are divided into the layer t. Nodes at layer t wake up at the $(T-t)$-th timeslot to receive data from the upper layer node and $(T-t+1)$-th timeslot to send data to the next hop with the allocated power in step 3).

In the proposed distributed algorithm, each node needs to calculate two parameters: routing weight $\sqrt{d^{\alpha}_{A_iA_{i+1}}}$ and transmission power P, and the computational complexity of each node is constant order, i.e., $O(1)$ time complexity.

IV. DOWNLINK TRANSMISSION PROCEDURE

During the downlink transmission, we choose a part of nodes based on EFMSS to broadcast the information to the whole network. At the same time, all nodes are divided into T hierarchy in the light of their hop numbers to the sink node and scheduled according to the downlink sleeping scheduling strategy to reduce energy consumption. In the next subsection, we will discuss the EFMSS in detail.

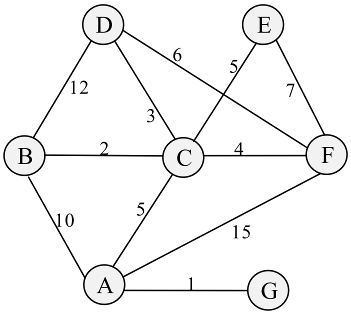


FIGURE 5. Example to illustrate different MPR set selection strategies.

TABLE 1. Node A's MPR(s).

MPR set selection mechanism	1-hop neighbours	2-hop neighbours	MPR(s)
CFMSS	B,C,F,G	D,E	C
EFMSS	B,C,F,G	D,E	B,F

A. ENERGY FIRST MPR SET SELECTION ALGORITHM (EFMSS)

In the traditional OLSR, a node selects a set of 1-hop neighbors that covers (in terms of radio range) all symmetric strict 2-hop nodes as MPRs to forward its messages. The principle for MPR set selection is to iteratively select a 1-hop neighbor which reaches the maximum number of uncovered 2-hop neighbors, which is called as coverage first MPRs set selection algorithm (CFMSS). Therefore, the 'energy-efficient' paths cannot be found by MPR selection mechanism. Fortunately, the proposed EFMSS can select the nodes with the largest residual energy to route the control messages. The purpose of this mechanism is to iteratively find one-hop neighbors with more residual energy to two-hop neighbors as MPRs until all the 2-hop neighbors are covered.

Fig. 5 is used to illustrate the proposed method. The selected MPRs for node A are shown in Table 1. Based on the definition of MPRs, a set of A's 1-hop neighbors is selected to cover all A's 2-hop neighbors as A's MPRs to relay the packets from A, while the 1-hop neighbors (not MPRs) don't need to retransmit the packet from A. Thus, both the overhead of control messages and the energy are reduced. According to Table 1, both D and E belong to A's 2-hop neighbors. Among A's 1-hop neighbors, B, C and F except G can serve as relays to reach all A's 2-hop neighbors. However, C is selected as A's MPR in CFMSS because it covers 5 neighbors while B and F only cover 3 and 4 neighbors, respectively, i.e., CFMSS chooses MPRs according to the coverage of nodes.

In our method, node A uses Dijkstra's or Bellman-Ford's algorithm to compute the heaviest 2-hop path to D. For node D, path AB $\oplus$ BD is the heaviest one, where $\oplus$ denotes the series connection. $W(\text{AB} \oplus \text{BD}) = 10 + 12 = 22$. Thus, B is firstly selected as A's MPR, and the 2-hop neighbour D is covered by the 1-hop neighbour B. Similarly, node A finds out the heaviest path to 2-hop neighbor E: A-F-E. The path weight is $W(\text{AF} \oplus \text{FE}) = 15 + 7 = 22$. So, F is selected as a MPR for relaying data from A to E. Until now, all A's 2-hop neighbors are reachable. This mechanism ensures that the best path to any node of A's 2-hop neighbors can be found. It is obvious that if C is chosen as the relay nodes as in OLSR, its energy will run out quickly. While EFMSS not only reduces the packet transmission number, but also balances network energy consumption, and eventually prolongs network lifetime. However, the new mechanism increases overheads because it increases the number of MPR in the network compared with CFMSS. But it is still superior to the flooding protocol and proven sustainable because a node has a small set of neighbors.

With the EFMSS, only the MPRs with relatively large residual energy need to retransmit the broadcasting packets from the sink node, and thus the optimal energy utilization can be realized. To further increase the lifetime of network, an energy threshold E-th is set. If the chosen MPR's energy declines to E-th, the MPR will send an alarm to the sink node, and the sink node will look for the substitution for this MPR, thus the MPR set will be renewed.

Based on the above discussion, the specific steps of EFMSS are described as follows:

1) The MPR set is chosen out for the first time using the CFMSS in OLSR because all nodes have the same energy at the initialization phase.
2) If any MPR's energy is less than the threshold E-th, start the MPR set selection process:
    a) Select the nodes with the largest residual energy as the MPRs until all the 2-hop neighbors are reachable.
    b) Iteratively select the MPRs until all nodes are reachable.
    c) When all the MPR nodes are selected, only the MPR set is responsible for retransmitting information and notifying the nodes in its communication range.
3) If any MPR's energy is less than the threshold E-th, go back to Step 2). If the Dijkstra's algorithm can not choose out an MPR set to cover all nodes in the network, stop the EFMSS algorithm network lifetime has expired.

B. DOWNLINK SLEEP SCHEDULING STRATEGY

In the downlink, each node uses Dijkstra's or Bellman-Ford's algorithm to compute the shortest path to the sink node and the layer is decided based on the distance to the sink node, i.e., if node is t-hop far away from the sink node, it is classified into the t-th layer. Although the same Dijkstra's or Bellman-Ford's algorithm is applied to obtain the hop number for both the uplink and downlink transmissions, the routing metric is different. Therefore, the same node may be located at different levels, such as node a in Fig. 1 and Fig. 2. Fig. 6 shows the hierarchical sleeping scheduling strategy for the downlink transmission. In the even duty cycle, all the nodes at level t periodically wake up at the $(t-1)$-th

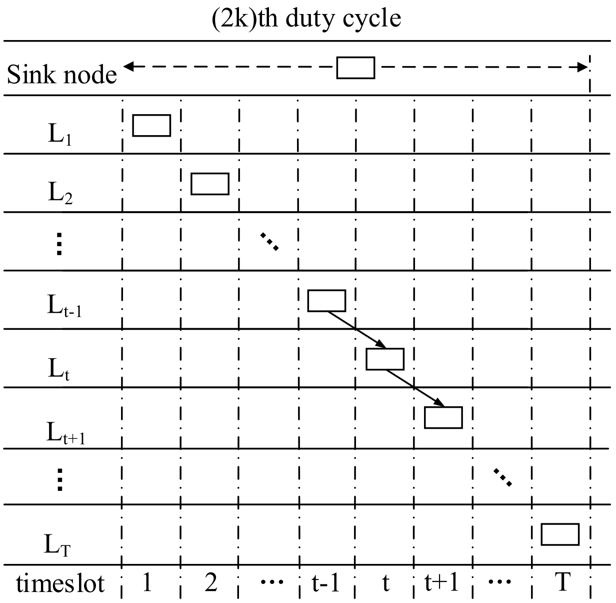


FIGURE 6. Hierarchical sleeping scheduling strategy for the downlink transmission.

TABLE 2. Simulation parameters.

simulation parameters	value
carrier frequency f_c	2.4 GHz
transmission bandwidth B	12 kHz
binary phase-shift keying modulation $(a : b)$	$(1 : 2)$
topology size	200 m × 200 m
source coordinate	$(11, 185)$
destination coordinate	$(100, 100)$
simulation topologies	1000
BER threshold ξ_{TH}	10^{-4}
legitimate node density λ_L	10^{-1}
eavesdropper density λ_E	10^{-4}
path loss factor α	2

timeslot to receive data from the upper layer and only the MPRs wake up at the t-th timeslot to send data to next layer. It is worth emphasizing that the nodes in each layer are comprised of MPRs and non-MPRs, only MPRs need to retransmit the packets from the upper layers.

V. SIMULATION RESULTS

In this part, we use MATLAB to simulate different algorithms. Firstly, we compare two kinds of MPR set selection algorithms EFMSS and CFMSS. Then, we evaluate the performance of three kinds of routing algorithms for the uplink transmission in WSNs: the proposed JPASR, FA [16] and SR [23]. Finally, we simulate the critical event reporting procedure in the proposed algorithm and EEDRINA algorithm [13]. The public simulation parameters are shown in Table 2.

A. COMPARISON OF EFMSS AND CFMSS

The traditional CFMSS selects the MPR nodes of each layer according to the principle of the nearest distance, while EFMSS takes both the coverage and energy into account. We randomly generate a topology with the simulation parameters in Table 2. The protocol interference model is used in the topology. Communication and interference distance are set as 40 and 50 meters respectively. Fig. 7 shows the network topology and the layer architecture of nodes computed according to the dijkstra's algorithm. Table 3 depicts the MPRs selection results for EFMSS and CFMSS. It shows that different selection algorithms choose different nodes as MPRs in each layer. Node C is selected as MPR in EFMSS because it has more residual energy than node B. The comparison process has been discussed elaborately in Section IV. The change of network lifetime with increasing network size under different selection algorithms are shown in Fig. 8. Compared with CFMSS, EFMSS can effectively improve network lifetime, because EFMSS takes the coverage and residual energy of nodes into account when selecting MPR nodes. Meanwhile, load balancing has been realized during this progress, so it can effectively prolong the lifetime of WSNs. While CFMSS only takes coverage as a condition of selecting MPRs, as a result, some backbone MPR nodes will exhaust its energy quickly, and thus CFMSS has a worse performance as compared with EFMSS.

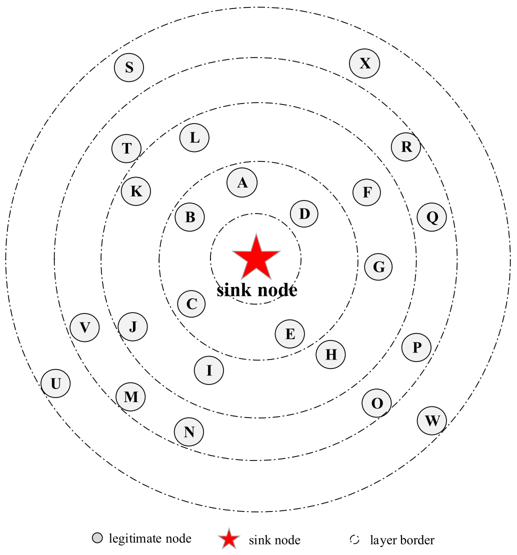


FIGURE 7. The network topology and the layer architecture of nodes.

TABLE 3. Node A's MPR(s).

MPR set selection mechanism	MPRs in each layer		
	Layer 1	Layer 2	Layer 3
CFMSS	B,C,D,E	F,H,I,L	M,P,Q,T
EFMSS	A,C,D,E	F,H,J,K	O,Q,T,V

B. COMPARISON OF DIFFERENT UPLINK ALGORITHMS

In this part, we compare JPASR with FA and SR algorithms in the following aspects: the average route transmission power consumption, the routing selection of different algorithms and RSCP. Specifically, FA algorithm prolongs the lifetime of sensor networks by finding the route and allocating the transmission power of nodes along the route. SR algorithm calculates the route with the maximal secure connection probability and do not consider the energy consumption.

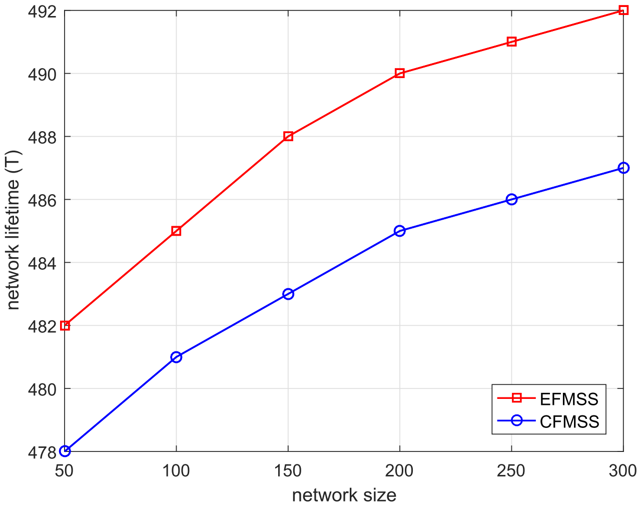


FIGURE 8. Network lifetime.

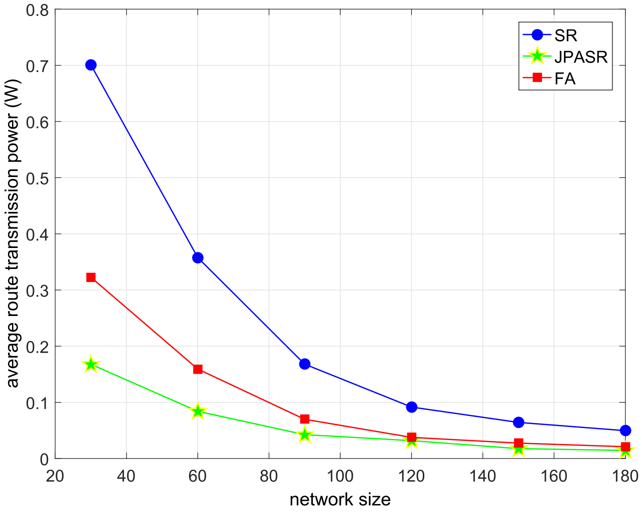


FIGURE 9. Average route transmission power consumption under different network sizes.

The results are averaged with 10000 simulation values. The transmission power in FA and JPASR are calculated according to (40) in [4] and (22) for different topologies. The transmission power in SR is set as the maximal transmission power in JPASR.

Fig. 9 simulates the average route transmission power consumption in different network sizes with three different algorithms. It can be seen that the average route transmission power consumptions in the three algorithms are all decreasing with respect to the growing number of nodes in the network. This is because, as the network size increases, the number of nodes in the selected routing path also increases, which makes the transmission distance between adjacent nodes closer and the power consumption smaller. As a result, the average route transmission power consumption are becoming smaller. As the number of nodes increases, the hop number in the routes selected by different algorithms is getting closer, so the gaps of power consumption are getting smaller. It is obvious that JPASR has the best performance than the others. JPASR finds a path with the least power consumption based on the network topology, while the transmission power along the route is redistributed at the same time, and the sleeping scheduling reduces the energy consumption further. FA only considers how to select a route that can escape from the special nodes with less energy to prolong the network lifetime. As a result, in order to keep away from these nodes, FA may choose a longer route to deliver the packet which induces large energy consumption. SR is the improved shortest path algorithm. It takes both hop number and node distance into consideration. So it takes less power to forward the packets than FA. However, its nodes use fixed power to retransmit packet and are always awake no matter whether they need to work, so the performance of SR is worse than that of JPASR.

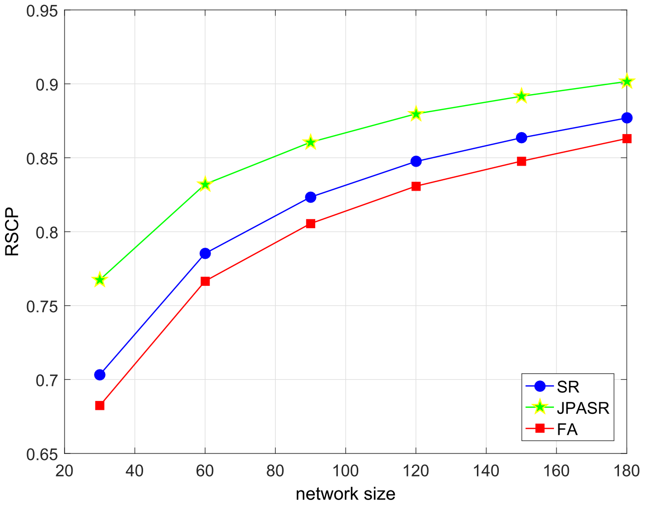


FIGURE 10. Routing secure connection probability in different network sizes.

Fig. 10 depicts how RSCP varies with the network size, and Fig. 11 shows a specific routing diagram. They are both simulations under the condition of $\xi_{\mathrm{TH}} = 10^{-4}$, $\lambda_E = 10^{-4}$. We can observe from Fig. 10 that RSCP of JPASR is better than those of FA and SR. Fig. 11 intuitively shows that the chosen routes by JPASR and SR effectively avoid eavesdropping to ensure the information transmission security. FA does not consider security, and the route it chooses is close to the eavesdroppers, so its RSCP is very low. When SR chooses the route, node transmission power is fixed, so it limits the algorithm to find a better route to avoid eavesdropping. While JPASR can coordinate the power allocation according to the distance between nodes to obtain an optimal configuration to maximize RSCP, it has the best secure performance.

Fig. 12 simulates RSCP under different eavesdropper densities. As eavesdropper density λ_E grows, the RSCP decreases. The gaps between JPASR and the other algorithms become larger and larger. This is because when there are less eavesdroppers, all algorithms are secure. However, as the eavesdropper density increases, the security cannot be guaranteed by all algorithms as before and only JPASR shows the best secure performance in the worse condition.

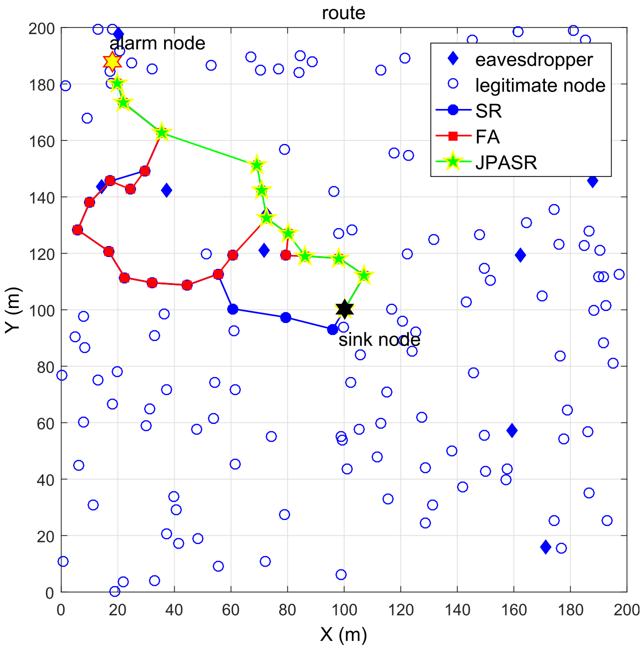


FIGURE 11. Uplink routing selection contrast diagram.

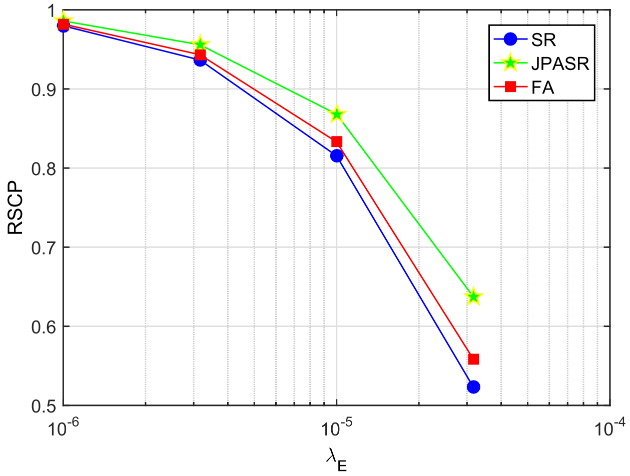


FIGURE 12. Routing secure connection probability under different eavesdropper densities λ_E.

C. SIMULATION OF TOTAL ENERGY COMSUMPTION

In this part, we simulate the average energy consumption for each critical event reporting procedure in different network sizes. We calculate the energy consumption by adding the consumption in the wake-up duration and the transmitting procedure. For example, when a MicaZ node turns on its radio module, its current is about 20 mA. Hence, the energy consumption within 5 ms wake-up duration is about 3.3V × 20mA × 5ms $=$ 3.3mJ. We capare our algorithm with the existing critical event reporting EEDRINA algorithm in [13]. EEDRINA selects a head node to aggregate the event data and then transmit to reduce the overhead. It is obviously that our algorithm needs less energy to finish a critical event reporting procedure in Fig. 13. EEDRINA uses the cluster head to collect the event data, and reduces the uplink overhead. However, it is more important to reduce the downlink overhead, and there is still a large number of messages that should be transmitted in the downlink. Furthermore, not only in the downlink but also in the uplink, every node is awake all the time. Therefore, EEDRINA wastes much more energy than our algorithm. When the network size increases, the gap is getting larger. In EEDRINA, the messages in the uplink transmission is reduced but those in the downlink transmission are doubled. In our algorithm, with the growing number of nodes in the same area, each MPR node can cover more nodes in its coverage area. Thus, the MPR strategy works better, and saves more energy.

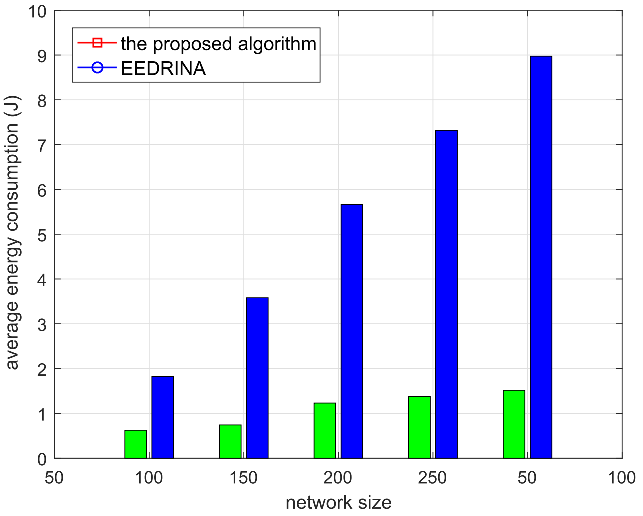


FIGURE 13. Average energy consumption for each critical event reporting procedure.

VI. CONCLUSION AND FUTURE DIRECTION

In this paper, a novel method is proposed for the critical event reporting in WSNs. The method has considered the information transmission security and the energy saving during the critical event reporting process. The simulation results show that our proposed method has good performance in the following respect: network lifetime, energy consumption and security index. Due to the implementability of MPRs strategy in a real WSN, we plan to apply the method to a WSN testbed to verify its performance in the future.

REFERENCES

[1] D. Eddine-Boubiche, J. A. Trejo-Sánchez, H. Toral-Cruz, J. L. López-Martínez, and F. Hidoussi, "Wireless sensor technology for intelligent data sensing: Research trends and challenges," in *Intelligent Data Sensing and Processing for Health and Well-Being Applications*. Amsterdam, The Netherlands: Elsevier, 2018, pp. 41–58.

[2] S. Boubiche, D. E. Boubiche, A. Bilami, and H. Toral-Cruz, "Big data challenges and data aggregation strategies in wireless sensor networks," *IEEE Access*, vol. 6, pp. 20558–20571, 2018.

[3] H. Ben Fradj, R. Anane, M. Bouallegue, and R. Bouallegue, "A range-based opportunistic routing protocol for wireless sensor networks," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 770–774.

[4] H. Rhim, K. Tamine, R. A. Bassi, D. Sauveron, and S. Guemara, "A multi-hop graph-based approach for an energy-efficient routing protocol in wireless sensor networks," *Hum.-Centric Comput. Inf. Sci.*, vol. 8, no. 1, pp. 30–38, 2018.

[5] K. H. Naik and V. R. Reddy, "Comparative performance of PRO-AODV, DFRR, CPRR algorithm based on link failure route rectification problem in mobile sensor network," *Int. Res. J. Eng. Technol.*, vol. 2, no. 9, pp. 2558–2564 , 2015.

[6] T. K. Jain, D. S. Saini, and S. V. Bhooshan, "Lifetime optimization of a multiple sink wireless sensor network through energy balancing," *J. Sensors*, vol. 2015, pp. 1–6, 2015.

[7] C. B. Vinutha, N. Nalini, and B. S. Veeresh, "Energy efficient wireless sensor network using neural network based smart sampling and reliable routing protocol," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2017, pp. 2081–2085.

[8] M. Zhao, Y. Yang, and C. Wang, "Mobile data gathering with load balanced clustering and dual data uploading in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 14, no. 4, pp. 770–785, Apr. 2015.

[9] A. Attiah, M. Chatterjee, and C. C. Zou, "A game theoretic approach for energy-efficient clustering in wireless sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[10] A. Attiah, M. F. Amjad, M. Chatterjee, and C. Zou, "An evolutionary routing game for energy balance in wireless sensor networks," *Comput. Netw.*, vol. 138, pp. 31–43, Jun. 2018.

[11] F. Hidoussi, H. Toral-Cruz, D. E. Boubiche, R. Martínez-Peláez, P. Velarde-Alvarado, R. Barbosa, and F. Chan, "PEAL: Power efficient and adaptive latency hierarchical routing protocol for cluster-based WSN," *Wireless Pers. Commun.*, vol. 96, no. 4, pp. 4929–4945, Oct. 2017.

[12] X. Liu, "An Optimal-Distance-Based transmission strategy for lifetime maximization of wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 6, pp. 3484–3491, Jun. 2015.

[13] Y. Y. Shinde and S. S. Sonavane, "An energy efficient critical event monitoring routing method for wireless sensor networks," *Int. J. Comput. Appl.*, vol. 114, no. 10, pp. 24–31, 2015.

[14] Z. Han, J. Wu, J. Zhang, L. Liu, and K. Tian, "A general self-organized tree-based energy-balance routing protocol for wireless sensor network," *IEEE Trans. Nucl. Sci.*, vol. 61, no. 2, pp. 732–740, Apr. 2014.

[15] G. Samara and M. Aljaidi, "Efficient energy, cost reduction, and qos based routing protocol for wireless sensor networks," 2019, *arXiv:1903.09636*. [Online]. Available: https://arxiv.org/abs/1903.09636

[16] X. Ning and C. G. Cassandras, "On maximum lifetime routing in wireless sensor networks," in *Proc. 48th IEEE Conf. Decis. Control (CDC)*, Dec. 2009, pp. 3757–3762.

[17] U. Jain and M. Hussain, "Wireless sensor networks: Attacks and countermeasures," in *Proc. 3rd Int. Conf. Internet Things Connected Technol. (ICIoTCT)*, 2018, pp. 26–27.

[18] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of Things security: Layered classification of attacks and possible countermeasures," *Electron. J. Inf. Technol.*, vol. 9, Dec. 2016.

[19] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.

[20] Z. E. Ankaralı, A. Fatih Demir, M. Qaraqe, Q. H. Abbasi, E. Serpedin, H. Arslan, and R. D. Gitlin, "Physical layer security for wireless implantable medical devices," in *Proc. IEEE 20th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Sep. 2015, pp. 144–147.

[21] H. Ben Fradj, R. Anane, and R. Bouallegue, "Opportunistic routing protocols in wireless sensor networks," *Wireless Pers. Commun.*, vol. 104, no. 3, pp. 921–933, Feb. 2019.

[22] P. Jadhav and R. Satao, "A survey on opportunistic routing protocols for wireless sensor networks," *Procedia Comput. Sci.*, vol. 79, pp. 603–609, Jan. 2016.

[23] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

[24] P. Gonizzi, P. Medagliani, G. Ferrari, and J. Leguay, "RAWMAC: A routing aware wave-based MAC protocol for WSNs," in *Proc. IEEE 10th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2014, pp. 205–212.

[25] J. G. Proakis, "Digital communication," in *Publishing House of Electronics Industry*. 2009.

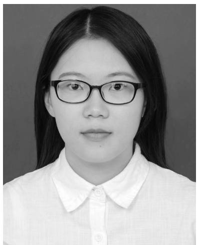
[26] Y. Chen and C. Tellambura, "Distribution functions of selection combiner output in equally correlated Rayleigh, Rician, and Nakagami-*m* fading channels," *IEEE Trans. Commun.*, vol. 52, no. 11, pp. 1948–1956, 2004.

[27] E. Morgado, I. Mora-Jimenez, J. J. Vinagre, J. Ramos, and A. J. Caamano, "End-to-End average BER in multihop wireless networks over fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2478–2487, Aug. 2010.

[28] P. Thulasiraman, J. Chen, and X. Shen, "Multipath routing and max-min fair QoS provisioning under interference constraints in wireless multihop networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 716–728, May 2011.

WEI FENG received the B.E. degree in electronics and information engineering from Hubei Engineering University, Xiaogan, China, in 2005, and the M.E. and Ph.D. degrees in communication and information systems from the South China University of Technology, Guangzhou, China, in 2009 and 2014, respectively. She has worked as an FAE with LITE-ON Technology Corporation, Guangzhou, and a Network Engineer with Huaxin Consulting Company Ltd., Hangzhou, China, from 2005 to 2006 and 2009 to 2011, respectively. She is currently a Lecturer with Hangzhou Dianzi University, Hangzhou. Her research interests include energy efficiency and physical layer security in future wireless communications.

FENG WANG was born in Yangquan, Shanxi, China, in 1996. She received the B.Eng. degree in communication engineering from HDU, Hangzhou, China, in 2019. She is currently working with HikVision Digital Technology Company Ltd., Hangzhou. Her current research interests include wireless networks optimization and distributed algorithm design.



DAN XU was born in Qingdao, Shandong, China, in 1995. She received the B.Eng. degree in communication engineering from Hangzhou Dianzi University (HDU), Hangzhou, China, in 2017, where she is currently pursuing the degree. Her current research interest includes wireless sensor networks optimization algorithm design.

YINGBIAO YAO was born in Songzi, Hubei, China, in 1976. He received the Ph.D. degree in communication and information system from Zhejiang University, Hangzhou, China, in 2006. He is currently a Professor with the School of Communication Engineering, Hangzhou Dianzi University, Hangzhou. His current research interests include SSD design, wireless sensor networks and indoor localization, and multimedia signal processing. He is also a member of the China Computer Federation (49541M).

XIAORONG XU (Member, IEEE) received the B.Eng. degree in communication engineering and the M.Eng. degree in communication and information system from Hangzhou Dianzi University (HDU), Hangzhou, China, in 2004 and 2007, respectively, and the Ph.D. degree major in signal and information processing from the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China, in 2010. From 2011 to 2013, he worked as a Postdoctoral Researcher with the Institute of Information and Communication Engineering, Zhejiang University (ZJU), Hangzhou. From 2013 to 2014, he has served as a Research Scholar with the Electrical and Computer Engineering Department, Stevens Institute of Technology (SIT), Hoboken, NJ, USA. He is currently an Associate Professor with the School of Communication Engineering, HDU. He is also an Excellent Backbone Teacher with HDU. His research interests include green wireless SWIPT networks, cognitive radio networks (CRN), cooperative communications, energy efficiency, physical layer security in SWIPT networks, and CRN.

XIANYANG JIANG received the M.Eng. degree in communication and information system from the Department of Electronic Engineering, Zhengzhou University, Zhengzhou, China, in 2004, and the Ph.D. degree in communication and information system from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2009. From July 2012 to December 2012, he has served as a Research Scholar with the Electrical and Computer Engineering Department, Stevens Institute of Technology (SIT), Hoboken, NJ, USA. Since 2009, he has been with the College of Telecommunication Engineering, Hangzhou Dianzi University (HDU), Hangzhou, China. His research interests include energy efficiency in broadband wireless communications, cognitive radio networks (CRN), and intelligent transportation.

MINGXIONG ZHAO received the B.S. degree in electrical engineering and the Ph.D. degree in information and communication engineering from the South China University of Technology (SCUT), Guangzhou, China, in 2011 and 2016, respectively. He was a Visiting Ph.D. Student with the University of Minnesota (UMN), Twin Cities, MN, USA, from 2012 to 2013, and the Singapore University of Technology and Design (SUTD), Singapore, from 2015 to 2016. Since 2016, he has been with the School of Software, Yunnan University, Kunming, China, where he is currently an Associate Professor. His current research interests include physical layer security, cooperative relay communication, and social aware communication systems.