IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received April 24, 2018, accepted May 24, 2018, date of current version June 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2841963

Fault-Tolerant Clustering Topology Evolution Mechanism of Wireless Sensor Networks

SHIHONG HU[1] **AND GUANGHUI LI**[1,2,3]

[1]School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, China
[2]Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China
[3]Engineering Research Center of Internet of Things Technology Applications, MOE, Wuxi 214122, China

Corresponding author: Guanghui Li (ghli@jiangnan.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61472368, in part by the Key Project of the Jiangsu Provincial Research and Development under Grant BE2016627, in part by the Fundamental Research Funds for the Central Universities under Grant RP51635B, and in part by the Wuxi International Science and Technology Research and Development Cooperative Project under Grant CZE02H1706.

ABSTRACT Wireless sensor networks (WSNs) are often subject to failures caused by energy depletion, software or hardware fault of nodes, environmental events, hostile attacks, and other reasons. It is critical to ensure a WSN application system is available during some presence of fault or interruption. Recent work in topology control has shown that a reasonable topology can improve the robustness of WSN. However, due to the limited resource of sensor nodes, topology control cannot easily tradeoff between fault tolerance and energy saving. To address this issue, we present a regular hexagonal-based clustering scheme (RHCS) and a scale-free topology evolution mechanism (SFTEM) for WSNs, which increases network survivability as well as maintains energy balance. RHCS uses a regular hexagonal structure for clustering sensor nodes, which satisfies at least 1-coverage fault-tolerance. SFTEM combines the reliability of RHCS with scale-free properties to connect clusters to form a robust WSN, which exploits the synergy between reliable clustering scheme and topology evolution, and can tolerate comprehensive faults including random failure and energy failure. In addition, to evaluate the performance of SFTEM, the simulation experiments were carried out to compare three factors including fault-tolerance, intrusion-tolerance, and energy balance with other methods in literature. The simulation results show that, the performance of SFTEM is superior to those of the referenced topology evolution mechanisms of WSNs.

INDEX TERMS Wireless sensor network, fault-tolerance, reliability, Markov model, scale-free.

I. INTRODUCTION

Wireless sensor networks (WSNs) are usually composed of a large number of distributed sensor nodes organized in an ad-hoc pattern to monitor environments [1], [2]. In many applications, it requires high coverage and reliability to accomplish rigorous monitoring tasks, such as military mission [3], volcanic monitoring [4], [5], and forest fire prevention [6], [7]. It further exacerbates the design challenge of meeting application requirements. WSNs always operate in unattended or hostile environments [8]–[10]. The sensor nodes in WSNs are easy to breakdown caused by energy depletion or natural disaster and deliberate attack [11], [12]. In addition, the failed sensor nodes would reduce the coverage of the network, would split originally connected network, and even lead to an entire global network paralysis. For example, if the several sensor nodes are breakdown and miss detecting the activity of the volcano malfunctions and gives fault readings, it might result in unneeded panic or loss of lives due to the absence of warning.

In order to ensure high quality of service, it is essential for a WSN to be able to detect its faulty sensor nodes before carrying out necessary recovery actions. Fault detection in WSN is a technique which identifies a fault when it occurred and pinpoints the type of fault and its location. Fault detection techniques can be classified into centralized, distributed and hybrid [13]. In centralized approach, many algorithms are based on machine learning techniques [14]–[27]. Distributed fault detection algorithms included neighborhood-based, probability-based, self-detection and cloud-based. Many distributed algorithms are proposed based on Bayesian model [18]–[20]. Hybrid algorithms are used in multi-tiered WSNs in which sensor nodes are organized into clusters with cluster heads (CHs). Clustering routing protocols have a variety of advantages, such as more scalability, less load, less energy consumption and more robustness [21]. Low-Energy Adaptive Clustering Hierarchy (LEACH) is one of the pioneering clustering routing approaches for WSNs. LEACH is to select sensor nodes as CHs by rotation, so the high energy dissipation in communicating with the base station is spread to all sensor nodes in the network. The basic idea of LEACH has been an inspiration for many subsequent clustering routing protocols, including Hybrid Energy-Efficient Distributed clustering (HEED), Two-Level Hierarchy LEACH (TL-LEACH) and Energy Efficient Clustering Scheme (EECS), etc.

Fault detection helps in isolating faulty sensors. Clustering routing scheme makes it more convenient for network topology control, and can respond to network changes composed of node's increasing and unpredicted failures. To solve the problem of random failure and hostile attack and energy depletion of sensor nodes in WSNs deployed in harsh environment, a robust topology can be designed to improve survivability of network. In this paper, we focus on studying reliable clustering scheme based on regular hexagonal structure, and fault-tolerant clustering topology evolution mechanism of WSNs, aiming to improve network fault tolerance and intrusion tolerance and energy balance.

A. RELATED WORK

Many mechanisms have been proposed for fault tolerance in WSNs to achieve reliability assurance, energy saving, and prolong the lifetime. Among them, node redundancy [22]–[24] is one of the important approaches. Korbi *et al.* [25] proposed a new fault-tolerant (FT) procedure to ensure both coverage and connectivity based on node redundancy. It is a proactive approach in the sense that it aims to replace the "up to fail" node before its defection. Mukhopadhyay *et al.* [26] proposed Markov models for WSNs reliability analysis. They also presented a reliability comparison for various numbers of defective nodes' replacements with hot-standby redundant nodes. Bein *et al.* [27] studied the coverage problem for WSNs from the fault-tolerance and reliability point of view. They proposed three 1-fault tolerant sensor deployment models. The placement of the sensors forms regular shapes, square or hexagonal. They also developed Markov models for each of the schemes and calculate their reliability. Munir *et al.* [28] modeled and analyzed fault detection and fault-tolerance in WSNs composed of duplex sensor nodes. They investigated the synergy between fault detection and fault-tolerance and use the fault detection algorithms' accuracies in their modeling of fault-tolerant WSNs.

Topology control is one of the critical factors which can influence the performance of WSNs. Xu *et al.* [29] investigated a dynamic topology control scheme to improve the network lifetime for WSNs in the presence of selfish sensors. A non-cooperative game aided topology control approach was developed for designing energy-efficient and energy balanced network topologies dynamically. Each sensor in the topology control game tried to minimize its unwillingness for constructing a connected network according to its transmission power. Albert and Barabasi [30] put forward the formation mechanism of power-law distribution in complex networks from the point view of dynamic and growing, which was called scale-free network, and constructed Barabasi-Albert (BA) model. The discovery of scale-free properties paves a new way to enhance the invulnerability of network topology. In scale-free WSNs, the small proportion of sensor nodes possesses most connections of the network, and most of the sensor nodes are low-degree, hence it has high resistance to random failure. Based on scale-free concepts and BA model, numerous studies have been devoted to promoting the structural robustness by designing the topology of the network. Zheng *et al.* [31] proposed a topology evolution model based on scale-free networks in theory. They not only considered the node fitness but also considered the node residual energy and node communication range of their practical evolution model, which improved the network energy balance and made the topology have a good robustness against random faults. Similarly, Liu *et al.* [32] presented a topology model with scale-free concepts and combined more characteristics of sensors, including residual energy, degree saturation, and maximum communication radius. The topology model improved energy efficiency as well as enhanced network robustness. Fu *et al.* [33] proposed a topology upgrading method by referencing the concept of a small word. Their scheme could improve the energy balance of the network significantly. Liu *et al.* [34] constructed a scale-free model which can assure the topological fault-tolerance against random faults and maximize topological intrusion-tolerance against selective remove attacks. The scaling exponent of degree distribution of the network can be adjustable.

B. CONTRIBUTIONS

The above mentioned studies show that the scale-free topology is robust to random failure but vulnerable to intrusion attack. In addition, in scale-free WSNs, a few key nodes possess most connections of network. The energy of these nodes will be depleted much faster than other nodes, thus threatening the normal operation of the entire network. To tolerate comprehensive faults and keep energy balance, we exploit the synergy between reliable clustering scheme and topology evolution. In this paper, we first construct a reliable clustering scheme of nodes and analyze its reliability based on the Markov model. And then, we present a scale-free topology evolution mechanism of WSNs. The contributions of this paper are:

1) A regular hexagonal-based clustering scheme (RHCS) with FT sensor nodes as the vertexes of the hexagon is constructed. We characterize the reliability and fault rate hierarchically at FT sensor node and RHCS using Markov model. Then we obtain the random failure probability (RFP) of RHCS.
2) We discuss the energy failure probability (EFP) of RHCS. Then we combine the RFP and EFP to model the JFP of RHCS. The relationship between the JFP and

its important parameters is analyzed by the mathematical method to prepare the theory for topology evolution mechanism.

3) A scale-free topology evolution mechanism (SFTEM) based on RHCS is presented. We treat a RHCS as an FT cluster, and evolve the topology based on the FT clusters. The connection strategy combines joint failure probability (JFP) and other characteristics of FT cluster, including node degree, node saturation and the distance between the cluster heads.
4) Comparison of simulation experimental results to demonstrate the superiority of the proposed SFTEM over the existing models.

In the remainder of this paper, Section II elaborates on the construction of RHCS. Section III models and analyzes the JFP of RHCS. Section IV describes our FT clustering topology evolution mechanism. Simulations and results are presented in Section V. Section VI concludes our study.

II. TRUCTION of RHCS

In this section, we first introduce the FT sensor node and analyze the failure rate using Markov method. Then, the RHCS with FT sensor nodes as the vertexes of the hexagon is established. Moreover, we investigate the relationship between the reliability of RHCS and the failure rate of FT nodes based on the Markov model. Finally, we exploit different initial state of RHCS and obtain the RFP.

A. FT SENSOR NODE

Node redundancy would be most effective to enhance the FT capability of sensor nodes. Hence, we refer the duplex sensor node as an FT sensor node [28]. In FT sensor node model, we assume that the redundant node is in a cold standby mode. The inactive node becomes active only when the active node is diagnosed faulty.

Definition 1 [Node Failure Rate λ_t (NIST [35]):] The failure rate of a sensor node can be expressed as an exponential distribution with a failure rate of λ_t over the time t_s.

$$p = 1 - e^{-\lambda_t t_s} \tag{1}$$

The exponential model works well for those inter-arrival times where the total number of events in a given time period is given by the Poisson distribution. When these events trigger failures, the exponential lifetime distribution model naturally applies [28].

Definition 2 [Node Degree k (Ismail and Mohamed [36])]: The degree of a node is the number of edges connected to the node.

Definition 3 [Coverage (Ammari and Habib [37])]: Coverage of an entire area otherwise known as full or blanket coverage means that every single point within the field of interest is within the sensing range of at least one sensor node.

Definition 4 (Fault Diagnosis Accuracy Factor c): Fault diagnosis accuracy factor c represents the probability that an active sensor node has been correctively diagnosed and replaced by a backup sensor node. Factor c depends on node degree k and the cumulative probability of sensor failure λ_t [28]. We model c ($c \leq 1$) with the empirical relation:

$$c = f(k) = \frac{k \times (1-\lambda_t)}{k^{(k/M(\lambda_t))^{1/M(\lambda_t)}+(1-k/M(\lambda_t))^k}}, \tag{2}$$

Where $M(\lambda_t)$ is the function of λ_t and denotes an adjustment parameter that may correspond loosely to the desired average node degree required to achieve a good fault detection accuracy for a given λ_t.

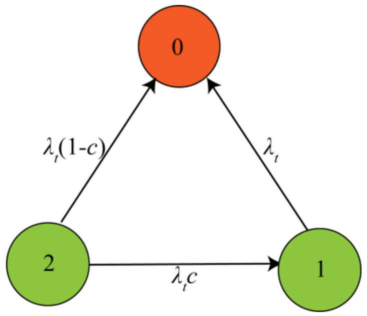


FIGURE 1. Markov model of FT sensor node (Munir *et al.* [28]).

The Markov model of the FT sensor node is depicted in Fig. 1. The states in the Markov model represent the number of good sensor nodes. State 1 and State 2 represent the active state, and State 0 means that sensor node is failed. When the active node falls to fail, the node will transfer State 2 to State 1 if the fault is correctly diagnosed, else the node will transfer to State 0; when the node in State 1 fails, the node will directly transfer to State 0. We finally obtain the average failure rate of the FT sensor node (See the details in [28]).

$$\lambda_{FT} = \frac{\lambda_t}{1+f(k)} \tag{3}$$

B. REGULAR HEXAGONAL-BASED CLUSTERING SCHEME

The sensing and transmission range of a sensor node are modeled as a disk of radius r_s and r_c, respectively. Zhang and Hou [38] have proved that if the ratio between the transmission range and the sensing range, denoted as r_{cs}, is not smaller than 2, then coverage implies connectivity. They have also shown that a regular triangular lattice pattern is optimal when the ratio $r_{cs} \leq \sqrt{3}$.

Definition 5 (k-Coverage Fault-Tolerance): If the node clustering scheme removes k nodes and still maintains the coverage of the scheme, the scheme is said to have k-coverage fault-tolerance.

FT sensor nodes are placed as shown in Fig. 2(a). The black contour disk is the sensing range of the common FT sensor nodes, and the radius of the disk is r_s. Six common FT nodes form a regular hexagonal structure. The strong FT node is located in the center of the hexagonal, whose sensing range is denoted as red contour disk and its radius of the disk is $\sqrt{3}\, r_s$. Furthermore, the distance d between adjacent FT nodes is all equal to $\sqrt{3}\, r_s$.

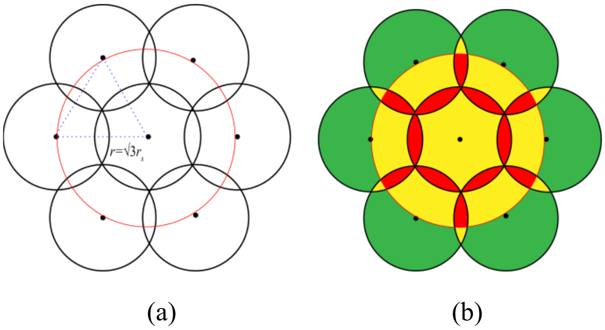


FIGURE 2. **Regular hexagonal-based clustering scheme: (a) Regular hexagonal structure of node clustering. (b) *k*-coverage fault-tolerance.**

As shown in Fig. 2(b), we analyze the k-coverage clustering scheme. According to Definition 4, we can get that the green area of the model represents 1-coverage fault-tolerance; the yellow area is 3-coverage fault-tolerance, and the red area expresses 5-coverage fault-tolerance. Therefore, the model meets at least 1-coverage fault-tolerance. We call this scheme regular hexagonal-based clustering scheme (RHCS).

C. RANDOM FAILURE PROBABILITY (RFP) ANALYSIS of RHCS

We make the following assumptions for the analysis of RFP of RHCS.

- When the strong FT node keeps operate properly, regardless of whether or not common FT nodes fail, RHCS is regarded as effective.
- When the strong FT node crashed but no common FT node fails, RHCS is considered effective;
- When the strong FT node crashed, once any common FT node fails, RHCS is considered breakdown.

Based on above assumptions, we exploit different initial state of RHCS and obtain the RFP.

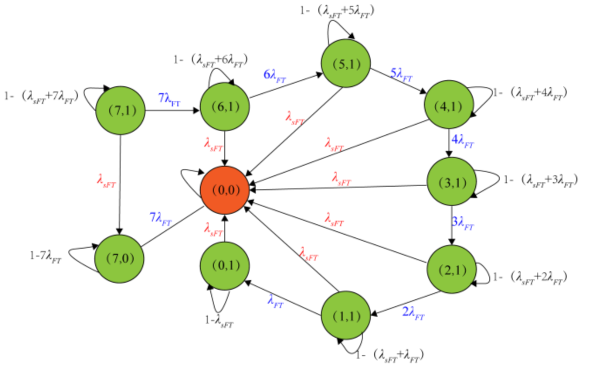

1- $(\lambda_{sFT}+5\lambda_{FT})$
1- $(\lambda_{sFT}+6\lambda_{FT})$
$6\lambda_{FT}$
(5,1)
$5\lambda_{FT}$
1- $(\lambda_{sFT}+7\lambda_{FT})$
$7\lambda_{FT}$
(7,1)
(6,1)
(4,1)
1- $(\lambda_{sFT}+4\lambda_{FT})$
λ_{sFT}
$4\lambda_{FT}$
(0,0)
(3,1)
1- $(\lambda_{sFT}+3\lambda_{FT})$
$7\lambda_{FT}$
$3\lambda_{FT}$
1-$7\lambda_{FT}$
(7,0)
(0,1)
(2,1)
1- $(\lambda_{sFT}+2\lambda_{FT})$
λ_{FT}
$2\lambda_{FT}$
(1,1)
1-λ_{sFT}
1- $(\lambda_{sFT}+\lambda_{FT})$

FIGURE 3. **Markov model of RHCS with no faulty nodes.**

1) RHCS FAULT-FREE IN INITIAL STATE

When the sensor nodes are fault-free in the initial state of RHCS, we use the Markov model to analyze the scheme reliability, as shown in Fig. 3. State '(7, 1)' means that all sensor nodes are operational, '7' means 7 common FT sensor nodes, '1' means the strong FT sensor node. When the strong FT node fails, the state is called '(7, 0)'; State '(6, 1)' represents that one of 7 common nodes fails, and the strong FT node is operational. When the entire model fails, the state is '(0, 0)'. The common FT node failure rate is λ_{FT}, and the failure rate of the strong FT node is λ_{sFT}.

The RFP of the model is the probability of the scheme to be in any failed states. Assuming $\lambda_{sFT} = \lambda_{FT}$, we obtain the RFP of the model depicted in Fig. 3 by solving the differential equation (See Appendix for more details):

$$P_F(t) = 1 - e^{-\lambda_{FT}t} - e^{-7\lambda_{FT}t} + e^{-8\lambda_{FT}t} \tag{4}$$

2) RHCS HAS ONE OR MORE FAULT NODES IN INNITIAL STATE

If the strong FT node fails in initial state of RHCS, we know that once any common FT node failure occurs again, RHCS is considered to be invalid. Its Markov model is shown in Fig. 4.

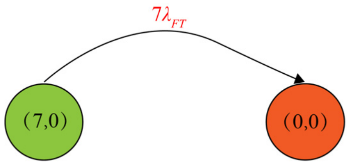


FIGURE 4. **Markov model of RHCS with strong FT node failure.**

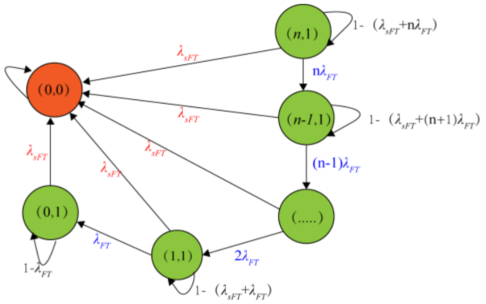


FIGURE 5. **Markov model of RHCS with strong FT node operational and common FT node failure.**

If the strong FT node is operational and the common FT node fails in initial state of RHCS, no matter how several faults occur, the Markov model can be represented as shown in Fig. 5. We obtain the RFP of the above model in Fig. 4 and Fig. 5 by solving the differential equation (See Appendix for more details):

$$P_F(t) = 1 - e^{-\lambda_{FT}t} \tag{5}$$

Where λ_{FT} is related to $f(k)$ (Equation.(3)), and $f(k)$ depends on the number of the faulty nodes in RHCS.

Combined with the above analysis, the RFP of RHCS can be divided into two cases:

- When the nodes are fault-free in the initial state of RHCS, the RFP of RHCS is shown in (4).

- When RHCS has any faulty nodes in its initial state, the RFP of RHCS is shown in (5).

III. MODELING AND ANALYSIS OF JOINT FAILURE PROBABILITY IN RHCS

In this section, we first discuss the energy failure probability (EFP) of RHCS. Then we combine the RFP and EFP to model the JFP of RHCS. Finally, the relationship between the JFP and its important parameters is analyzed by the mathematical method to prepare the theory for topology evolution in the next section.

A. ENERGY FAILURE PROBABILITY (EFP)

We adopt the classic First-order radio energy consumption model of wireless communication in our paper. The energy consumption of sending a l-bit message is $E_{tx} = E_{elec} \cdot l + \varepsilon_{amp} \cdot l \cdot d^2$, where E_{elec} is data fusion energy consumption, ε_{amp} is amplifier power consumption, and d is the transmission radius of the node. The energy consumption of receiving a one-bit message is $E_r = E_{elec} \cdot l$. So the total energy consumption of the node is $E_c = E_{tx} + E_r$.

For RHCS, the basic structure of the scheme is a regular hexagon. If the topology is evolved based on RHCS, then the energy consumption will have little difference among the clusters. Therefore, considering the actual deployment requirements, the size of RHCS will change according to the distance d, as shown in Fig. 6, where $d \in [\sqrt{3}\, r_s, 2r_s]$.

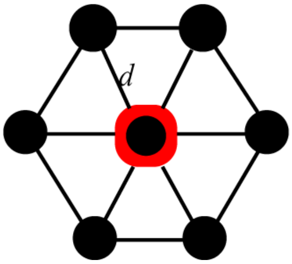


FIGURE 6. The basic structure of the RHCS.

According to the energy model above, we obtain the total energy consumption of RHCS:

$$E_c = n_c \cdot E_{nc} = 2n_c \cdot E_{elec} \cdot l + n_c \cdot \varepsilon_{amp} \cdot l \cdot d^2 \tag{6}$$

Where n_c is the number of nodes in RHCS that are operational.

If the initial energy of RHCS is E_0, the EFP of the model can be described as (Mizanian *et al.* [39]):

$$P_e = 1 - e^{\frac{-E_c}{E_0} t} \tag{7}$$

According to (7), P_e can also be written as:

$$P_e = 1 - e^{-(A+B\cdot d^2)t} \tag{8}$$

where $A = \frac{2n_c \cdot E_{elec} \cdot l}{E_0}$, $B = \frac{n_c \cdot \varepsilon_{amp} \cdot l}{E_0}$.

B. JOINT FAILURE PROBABILITY (JFP)

Combining the RFP and EFP of RHCS, the joint failure probability (JFP) of the model is established.

- When the nodes are fault-free in the initial state of RHCS, the JFP is described as:

$$P = (1 - e^{-(A+B\cdot d^2)t})(1 - e^{-\lambda_{FT} t} - e^{-7\lambda_{FT} t} - e^{-8\lambda_{FT} t}) \tag{9}$$

- When RHCS has any faulty nodes in the initial state, the JFP is defined as:

$$P = (1 - e^{-(A+B\cdot d^2)t})(1 - e^{-\lambda_{FT} t}) \tag{10}$$

1) QUALITATIVE ANALYSIS OF JFP

Definition 6 (Comprehensive Demand): For RHCS, t_{min} is the minimum running time of the cluster, $f(k)_{min}$ and $f(k)_{max}$ are the minimum and maximum of the node degree function. If the cluster satisfies $t \geq t_{\min}$, all the nodes in the cluster satisfy $f(k)_{\min} \leq f(k) \leq f(k)_{\max}$ and the distance between adjacent nodes follows $d_{\min} \leq d \leq d_{\max}$, then RHCS is called to meet the comprehensive demand of lifetime and JFP.

Theorem 1: In RHCS, if the JFP satisfies

$$\begin{aligned} P = (1 - e^{-(A+B\cdot d_{\max}^2)t_{\min}})(1 - e^{-\frac{\lambda_t}{1+f(k)_{\min}} t_{\min}} \\ - e^{-7\frac{\lambda_t}{1+f(k)_{\min}} t_{\min}} + e^{-8\frac{\lambda_t}{1+f(k)_{\min}} t_{\min}}) \end{aligned} \tag{11}$$

or

$$P = (1 - e^{-(A+B\cdot d_{\max}^2)t_{\min}})(1 - e^{-\frac{\lambda_t}{1+f(k)_{\min}} t_{\min}}), \tag{12}$$

then RHCS meets the comprehensive demand.

Proof: For simplicity, we prove that if the JFP satisfies (12), then RHCS meets the comprehensive demand.

According to the condition $t \geq t_{\min}$, we get

$$P \geq (1 - e^{-(A+B\cdot d^2)t_{\min}})(1 - e^{-\frac{\lambda_t}{1+f(k)} t_{\min}}) \tag{13}$$

Since $f(k)_{\min} \leq f(k) \leq f(k)_{\max}$ and $d_{\min} \leq d \leq d_{\max}$, we have

$$\begin{aligned} &(1 - e^{-(A+B\cdot d_{\min}^2)t_{\min})})(1 - e^{-\frac{\lambda_t}{1+f(k)_{\max}} t_{\min}}) \\ &\leq (1 - e^{-(A+B\cdot d^2 t_{\min})})(1 - e^{-\frac{\lambda_t}{1+f(k)} t_{\min}}) \\ &\leq (1 - e^{-(A+B\cdot d_{\max}^2)t_{\min})})(1 - e^{-\frac{\lambda_t}{1+f(k)_{\min}} t_{\min}}) \end{aligned} \tag{14}$$

Based on (13) and (14), it can be deduced that

$$P \geq (1 - e^{-(A+B\cdot d_{\max}^2)t_{\min}})(1 - e^{-\frac{\lambda_t}{1+f(k)_{\min}} t_{\min}}) \tag{15}$$

Since $f(k)_{\min} \leq f(k) \leq f(k)_{\max}$ and $d_{\min} \leq d \leq d_{\max}$, we get

$$\begin{aligned} (1 - e^{-\frac{\lambda_t}{1+f(k)_{\max}} t}) &\leq (1 - e^{-\frac{\lambda_t}{1+f(k)} t}) \\ &\leq (1 - e^{-\frac{\lambda_t}{1+f(k)_{\min}} t}) \\ (1 - e^{-(A+B\cdot d_{\min}^2)t}) &\leq (1 - e^{-(A+B\cdot d^2)t}) \\ &\leq (1 - e^{-(A+B\cdot d_{\max}^2)t}) \end{aligned} \tag{16}$$

Then, we deduce

$$(1-e^{-(A+B\cdot d_{\min}^2)t})(1-e^{-\frac{\lambda_t}{1+f(k)_{\max}}t}) \le P \\ \le (1-e^{-(A+B\cdot d_{\max}^2)t})(1-e^{-\frac{\lambda_t}{1+f(k)_{\min}}t}) \quad (17)$$

Because $t \ge t_{\min}$, we have

$$(1-e^{-(A+B\cdot d_{\max}^2)t_{\min}})(1-e^{-\frac{\lambda_t}{1+f(k)_{\min}}t_{\min}}) \\ \le (1-e^{-(A+B\cdot d_{\max}^2)t})(1-e^{-\frac{\lambda_t}{1+f(k)_{\min}}t}) \quad (18)$$

Then, we obtain

$$P \le (1-e^{-(A+B\cdot d_{\max}^2)t_{\min}})(1-e^{-\frac{\lambda_t}{1+f(k)_{\min}}t_{\min}}) \quad (19)$$

Based on (19) and (23), we get

$$P = (1-e^{-(A+B\cdot d_{\max}^2)t_{\min}})(1-e^{-\frac{\lambda_t}{1+f(k)_{\min}}t_{\min}}) \quad (20)$$

When the JFP of RHCS satisfies (14), denoted as P_0, the model can meet the comprehensive demand of lifetime and joint fault-tolerance.

2) QUANTITATIVE ANALYSIS OF JFP

The above qualitative analysis transforms the comprehensive demand of network's lifetime and joint fault-tolerance into the requirement of network's JFP. By quantitative analysis of JFP, we obtain the relationship between the node degree function $f(k)$ and the distance d between adjacent nodes with the maximum lifetime satisfying $P = P_0$ for JFP of network, which is shown in (20).

We transform (20) into the following formula:

$$P = F(d,t)G(f(k),t) \quad (21)$$

where $F(d,t) = (1-e^{-(A+B\cdot d^2)t})$, $G(f(k),t) = (1-e^{-\frac{\lambda_t}{1+f(k)}t})$, where $d_{\min} \le d \le d_{\max}$ and $f(k)_{\min} \le f(k) \le f(k)_{\max}$.

Then, Equation (20) can be described as

$$P_0 = F(d_{\max}, t_{\min})G(f(k)_{\min}, t_{\min}) \quad (22)$$

When d or t increases, function $F(d,t)$ increases, so we know that function $F(d,t)$ has a positive correlation with both d and t, and when d takes the minimum value, t will take the maximum value $t_{\max 1}$ to keep the F_0 unchanged; when $f(k)$ increases, function $G(f(k),t)$ decreases; and when t increases, function $G(f(k),t)$ increases, so we call that function $G(f(k),t)$ is negatively correlated with$f(k)$ and positively correlated with t, when $f(k)_{\max}$ takes the maximum value, t will also take the maximum value $t_{\max 2}$ to keep G_0 constant. We compare the value of $t_{\max 1}$ and $t_{\max 2}$:

- If $t_{\max 1} > t_{\max 2}$, we get $d = d_{min}$ and $f(k) = -\frac{t_{\max 1}\times\lambda_t}{\ln(1-F_0)} - 1$, RHCS will have the maximum lifetime.
- If $t_{\max 2} > t_{\max 1}$, we get $f(k) = f(k)_{\max}$ and $d_0 = \sqrt{\frac{C-A}{B}}$, where $C = -\frac{\ln(1-G_0)}{t_{\max 2}}$ and the value of A and B defined in (8), RHCS will have the maximum lifetime.

IV. TOPOLOG Y EVOLUTION MECHANISM AND DYNAMIC CHARACTERISTIC ANALYSIS

As a kind of energy-constrained distributed network, WSNs tend to adopt clustering structure in many cases to prolong the lifetime of the network. WSNs have obvious dynamic characteristics, including the increase of new nodes and new links, and the node failures caused by environmental factors or energy depletion. In this section, we evolve the scale-free topology based on the reliable distribution of cluster heads of FT clusters. Here, the process of evolution refers to the addition of new FT cluster heads to the network. Sensor nodes in the network are divided into strong FT nodes and common FT nodes. The common FT nodes join the network as in-cluster members of FT clusters and establish communication with the fixed cluster heads of FT clusters. When the strong FT nodes as cluster heads join the network, they will establish links with the cluster heads of other FT clusters, and use multi-hop communication to transmit the data.

A. CLUSTERING SCALE-FREE TOPOLOGY EVOLUTION MECHANISM

When a new cluster head joins the network, the JFP of the FT cluster, denoted as P, the degree k of cluster head and the distance D between cluster heads are taken as the evaluation criteria. Let the fitness function F be the reciprocal of the product of the P and D between the cluster heads. The probability of existing cluster head in the network being selected to connect with the new added cluster head depends on the value of F and k. Meanwhile, we set the threshold of k as k_{max}, it means that the maximum connection number of cluster head cannot exceed k_{max}. Specific evolution rules are as follows:

1) Network initialization: At initial time $t = 0$, the initial network consists of m_0 FT clusters and e_0 edges, and at least one edge of cluster heads of each FT cluster is connected with other cluster heads.
2) Preferential growth connection: At each time interval, one FT cluster head is added, m cluster heads of the existing FT cluster are selected to connect, and adding FT nodes in the cluster based on the structure of RHCS to form a new FT cluster. The probability $\prod k_i$ represents that an existing FT cluster head is selected to be connected obeys the following rule:

$$\prod k_i = (1 - \frac{k_i}{k_{\max}})\frac{F_i \times k_i}{\sum_{j\in\Omega} F_j \times k_j} \quad (23)$$

Where $F_i = 1/P(i) \times D_i$, k_i is the node degree of the cluster node of FT cluster i, $P(i)$ is the JFP of the i^{th} FT cluster, and D_i is the distance between the new cluster head and the cluster head of i^{th} FT cluster. Obviously, according to the connection rules, when the node degree of the FT cluster head is k_{max}, the probability of the FT cluster being selected to connect is zero.

The fitness function F combines the JFP with the distance between cluster heads of FT clusters, which considers the integrated failure probability of the FT clusters to be selected, including the RFP and EFP, and controls the energy consumption of the cluster head; that is, the smaller the distance is, the lower the energy consumption is. Meanwhile, k_{max} affects the distribution of k and the energy balance of the network.

B. DYNAMIC CHARACTERISTICS ANALYSIS

With the mean-field theory (Barabási *et al.* [40]), we analyze the distribution of k in the network. Assuming that the node degree k_i is continuous changing, and thus the probability can be considered as a continuous rate of change of k. Consequently, we get the dynamic equation for node i as follows:

$$\frac{\partial k_i}{\partial t} \approx m \prod k_i = m(1 - \frac{k_i}{k_{\max}}) \frac{F_i \times k_i}{\sum_{j \in \Omega} F_j \times k_j} \tag{24}$$

The distribution of k in the network has obvious heterogeneity according to the generation mechanism, which means that a few cluster heads account for most of the connections in the network, and the majority of nodes only have small proportion of the connections. Therefore, we get $(1 - \frac{k_i}{k_{\max}}) \approx 1$ under the condition of ensuring sufficient scale of the network. For the local-world Ω composed of M cluster heads, we have

$$\sum_{j \in \Omega} F_j \times k_j = M \overline{F} \tilde{k} t \tag{25}$$

Where $\overline{F}$ is the expectation of fitness, and $\tilde{k}$ represents the average node degree of the local world cluster heads. By the preferential connection rules, the network adds mt links after t time intervals, and each link connects two nodes, so the newly added node degree is $2mt$.

$$< k >= \frac{2mt}{m_0 + t} \approx 2m \tag{26}$$

After substituting (26) and (25) into (24), we get

$$\frac{\partial k_i}{\partial t} = \frac{F_i k_i}{2mM\overline{F}t} \tag{27}$$

Since $k_i(t = t_i) = m$, the (31) can be simplified as follows.

$$\frac{\partial k_i}{\partial t} = \frac{F_i}{2M\overline{F}t} \tag{28}$$

Solving (28), we get

$$k_i(t) = m(\frac{t}{t_i})^{\beta} \tag{29}$$

Where $\beta = \frac{F_i}{2M\overline{F}}$, thus the probability that a cluster head has a connectivity smaller than $k_i(t)$ is:

$$p(k_i(t) < k) = p\left(t_i > \left(\frac{m}{k}\right)^{\frac{1}{\beta}}\right) = 1 - \frac{t}{m_0 + t}\left(\frac{m}{k}\right)^{\frac{1}{\beta}} \tag{30}$$

The probability of density $p(k)$ can be obtained using

$$\begin{aligned} p(k) &= \frac{\partial p\,(k_i(t) < k)}{\partial k} = \lim_{t \to 0} \frac{t}{m_0 + t} \frac{1}{\beta} m^{\frac{1}{\beta}} k^{-\left(\frac{1}{\beta}+1\right)} \\ &= \frac{1}{\beta} m^{\frac{1}{\beta}} k^{-\left(\frac{1}{\beta}+1\right)} \end{aligned} \tag{31}$$

Consequently, we conclude that node degree distribution $p(k)$ of cluster head conforms to the power law distribution and the law exponent is $\gamma = 1/\beta + 1$. Therefore, the network generated by the SFTEM satisfies the characteristics of the scale-free network, and has the fault-tolerance of the scale-free network.

TABLE 1. Simulation parameters.

Parameter	Value
Deployment area	500m×500m
Number of cluster head C_{num}	160
Sink node coordinates	(250,250)m
Initial energy of strong FT node E_{c0} (J)	3
Initial energy of FT node E_{n0} (J)	1
Sensing radius r_s (m)	10
Transmission radius r_c (m)	100
Transmission data L (bit)	100
Data fusion energy consumption E_{elec} (nJ/bit)	50
Amplify power consumption ε_{amp} (pJ/bit/m^2)	100

V. SIMULATION AND ANALYSIS

We use the Matlab simulation tool to verify the theoretical results and the performance of SFTEM in this study. Assuming that sensor nodes are randomly deployed in a two-dimensional plane region, the initial energy of nodes is the same. In the initial network, the number m_0 of FT clusters is 4, and the connection number of newly added cluster heads denoted as m, is set to 2. To exclude errors caused by randomness, every experimental result is an average of 50 times simulation. The network parameters are shown in Table 1.

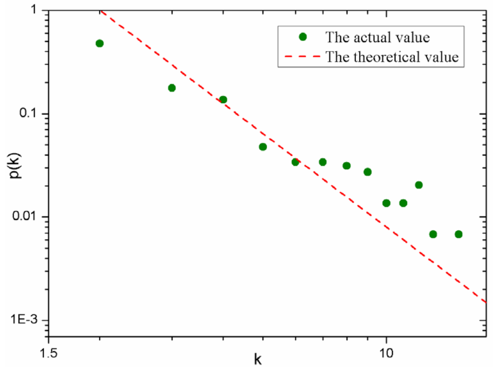


FIGURE 7. Degree distribution comparison

A. NODE DEGREE DISTRIBUTION OF SFTEM

In each generated topology by the SFTEM, we evaluate the degree distribution of the FT cluster head of the network. After 50 runs of simulation, we obtain the average values of these 50 results, as shown in Fig. 7. Meanwhile, in order to evaluate the influence of node degree threshold k_{max} on the SFTEM, k_{max} takes four different values of 15, 20, 25 and 30 to analyze the distribution of node degree respectively, the results are given in Fig. 8.

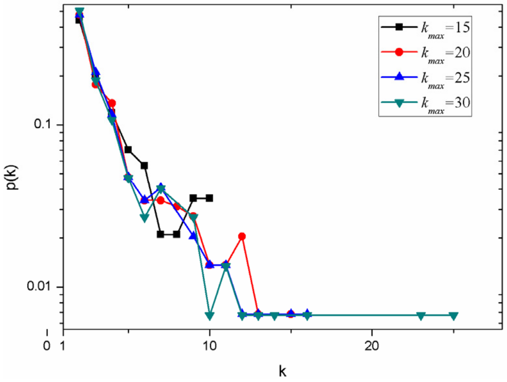


FIGURE 8. Degree distribution for different k_{max}.

As expected, Fig. 7 shows that the actual degree distribution is basically consistent with the theoretical distribution, thus the network topologies generated by SFTEM have the characteristics of scale-free networks, and can meet the robustness requirements in harsh environments. Moreover, Fig. 8 depicts that the heavy-tailed phenomenon in the degree distribution enhanced with the increase of k_{max} obviously. Therefore, by limiting the maximum degree of the FT cluster nodes, the degree heterogeneity of the network can be reduced, and the energy consumption balance can also be improved, so as to prolong the lifetime of network. To achieve a tradeoff between the performance of fault-tolerance and energy consumption, we take $k_{max} = 20$ as the parameter of the following simulation.

B. RELATIONSHIP BETWEEN LIFETIME AND f (k) AND d

Equation (2) demonstrates that $f(k)$ is correlated with node failure rate λ_t, the failure rate empirical function $M(\lambda_t)$, and node degree k. Because the number m of links of the newly added cluster heads is set to 2, the minimum degree k of the cluster head is 2. The values of $f(k)$ $(k = 2, 6, 10, 14, 18, 20)$ are shown in Table 2.

TABLE 2. Estimated values of $f(k)$.

		k					
λ_t	$M(\lambda_t)$	2	6	10	14	18	20
0.05	25	0.70	1.01	1.03	1.01	0.99	0.98
0.1	50	0.63	0.89	0.96	0.96	0.95	0.95
0.3	65	0.49	0.68	0.73	0.74	0.74	0.74
0.6	68	0.28	0.39	0.42	0.42	0.42	0.42
0.9	71	0.28	0.39	0.42	0.42	0.42	0.42

Table 2 shows the fault diagnosis accuracy factor $c\ (f(k))$ decreases with the increase of node failure rate λ_t. Particularly, if $\lambda_t \geq 0.1, f(k)$ is less than 1 for any k. Therefore, λ_t is taken as 0.05 in the following simulation. It can be seen that $f(k)_{\min} = 0.7$ and $f(k)_{\max} = 1.03$ from Table 2. To observe the relationship between $f(k)$ and k more clearly, we plot a graph of the curve between $f(k)$ and k as shown in Fig. 9. Fig. 9 reveals the fact that when $k \in [6, 15], f(k) \geq 1$, which means that once the node fails, it can be successfully replaced by the backup node.

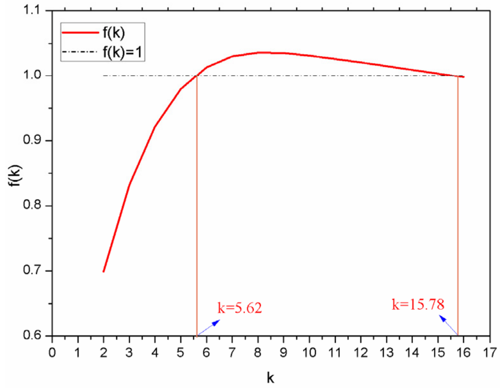


FIGURE 9. The curve of $f(k)$.

From the quantitative analysis of JFP in section III, if $f(k)_{\min} = 0.7$ and $f(k)_{\max} = 1.03$, then $t_{\max 2} > t_{\max 1}$, and $d_0 = 1.97r_s$. So, when $f(k) = f(k)_{\max}, d = d_0$, the FT cluster will have a maximum lifetime. Next, we design four simulations of topology evolution with different parameters to verify the relationship between network lifetime and $f(k)$ and d. The initial network of the four simulations is the same except that $f(k)$ of FT clusters and the distance d between adjacent nodes in the cluster during topology evolution. By controlling the number of failure nodes in the FT cluster, the values of $f(k)$ of sixty percentage of FT cluster are different, including $f(k)_{\max}$ and $f(k)_{\min}$. At the same time, the distance d between adjacent nodes in the FT cluster is also set to different values, including $d_{\max}$, $d_{\min}$, and d_0. Fig. 10 shows the lifetime comparison of four simulations, where lifetime is defined as the time of energy exhaustion of the first node in the network [41].

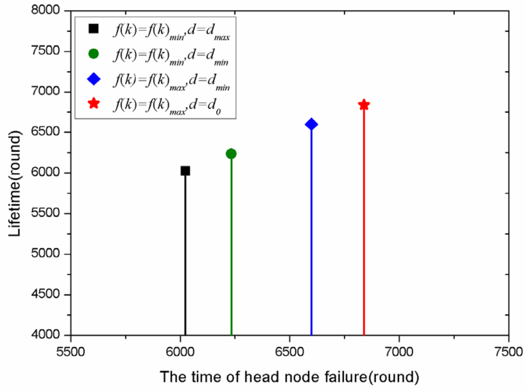


FIGURE 10. Comparison of lifetime.

The results shown in Fig. 10 demonstrate that when $f(k) = f(k)_{\max}, d = d_0$, the network lifetime is the longest of the four simulations. It well validates the theoretical results presented in section III. These results reveal that the lifetime of the network prolonged with the increase of $f(k)$. Obviously, when the distance d between adjacent nodes in the FT cluster increases, the energy consumption of the data transmission increases, which decreases the lifetime of the network. However, the JFP increases with the increases of d. d_0 is the compromise theoretical value that makes the lifetime achieve the optimal value. Therefore, the following simulations will take $f(k) = f(k)_{\max}$, $d = d_0$ as parameters of the topology evolution.

C. FAULT-TOLERANCE AND INTRUSION-TOLERANCE COMPARISON

To evaluate the fault-tolerance and intrusion-tolerance of RHCS topology, we compare the traditional BA model, Model 1 [32] and Model 2 [34], Model 1 has the advantage of energy balance, and Model 2 has the stronger network fault-tolerance and intrusion-tolerance. The initial network of the four topology evolution mechanism is the same, and the simulation parameters are all referenced in Table 1. In the fault- tolerance comparison simulation, the failure nodes are generated randomly according to Poisson distribution. The failure nodes are removed after each simulation time. We use C to denote the number of nodes in the maximum connected component to measure the fault-tolerance and intrusion-tolerance of topology.

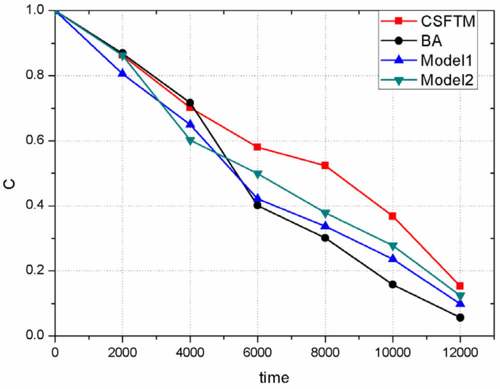


FIGURE 11. Comparison of fault-tolerance.

Fig. 11 shows the comparison among the fault-tolerance of four topologies. Before 4000 simulation times, C of BA topology is slightly bigger than SFTEM topology, because the BA model only considers the node degree in its topology evolution, it can achieve the optimal fault-tolerance. However, the availability of BA topology is low due to failure to consider energy balance [42], so when the simulation time exceeds 4000, the fault-tolerant performance of BA model is becoming poor, as shown in Fig. 11. Fig. 11 also shows that C of SFTEM topology is bigger than that of Model 1 and Model 2 at each simulation time, it indicates that SFTEM topology can better ensure the network connectivity in the case of a comprehensive failure, and it has a strong fault-tolerance against the comprehensive fault. SFTEM considers the impact of comprehensive fault on network fault-tolerance so that the results of SFTEM topology show better robustness for the energy exhaustion and random failure of nodes.

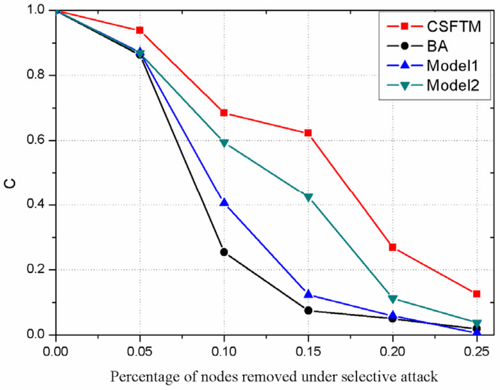


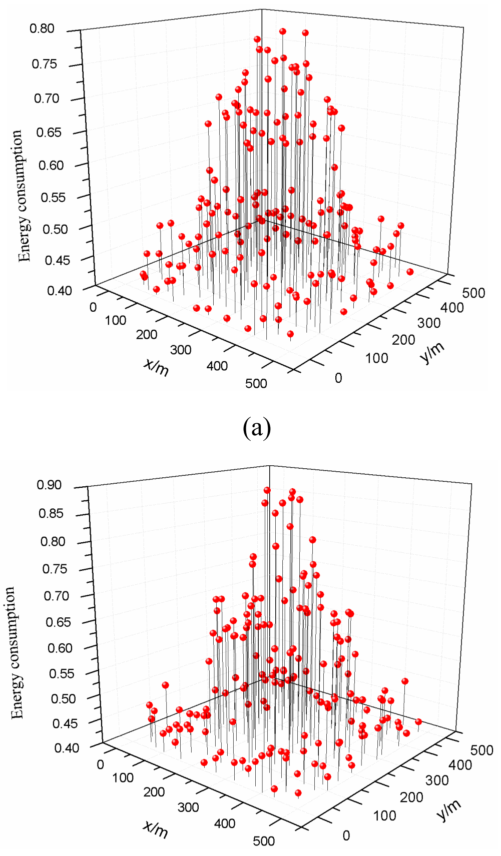
FIGURE 12. Comparison of intrusion-tolerance.

In the intrusion-tolerance simulation, we randomly remove the cluster heads with high degree, and the removal ratio ranged from 0.05 to 0.25. Fig. 12 displays the comparison of intrusion-tolerance of four topologies. From Fig. 12, we know that SFTEM has the strongest capacity against deliberate attack. When the percentage of nodes removed under selective attack is 0.15, C of SFTEM is up to 0.65, and Model 2 also maintains good intrusion-tolerance, C of which can keep 0.425. However, C of Model 1 is 0.123 and BA model is only 0.075 which means the network is almost paralysis; when the percentage of nodes removed reaches 0.25, C of SFTEM is still 0.125, and C of other three models approaches 0. Because SFTEM considers the factor of FT cluster energy consumption and node saturation, its degree distribution is more uniform, thus the topologies evolved by SFTEM have a good intrusion-tolerance. Model 2 can change the power-law scaling exponent by adjusting its parameter, so the degree distribution can be adjusted and to improve the intrusion-tolerance of the network [34].

D. COMPARISON OF ENERGY BALANCE

Let EC represent the ratio of node energy consumption to the initial energy. The higher EC is, the greater the energy consumption is. And the smaller difference of EC of cluster heads means that the more balanced energy consumption distribution of the network. We compare SFTEM with Model 1, for Model 1 considering the residual energy of nodes in its evolution rules. Fig. 13 displays the energy consumption distribution of the network of SFTEM topology and Model 1 topology.

As shown in Fig. 13, in both network topologies, the area near the sink node is the high energy-consuming area. Compared with Model 1, energy consumption of SFTEM is more uniform than that of Model 1. In SFTEM, the highest EC



(a)

(b)

FIGURE 13. **Energy consumption distribution: (a) RHCS. (b) Model 1.**

is 0.755 and the maximum difference of *EC* among the cluster heads around the sink node is about 0.12. However, the highest *EC* is 0.875 in Model 1 and the difference among the cluster heads around the sink node is relatively big, even the maximum of the difference of *EC* is higher than 0.2.

VI. CONCLUSIONS

WSNs are susceptible to failure due to the vulnerability of sensor nodes and attacks from malicious intruders. Hence, the fault-tolerance is an important issue in WSN applications. In this paper, we construct a regular hexagonal-based clustering scheme (RHCS) of sensor networks and analyze the reliability of RHCS based on Markov model. Then, we present a scale-free topology evolution mechanism (SFTEM). We also analyze the dynamic characteristics of SFTEM using mean-field theory. Simulation results show that the node degree distribution of SFTEM follows a power law distribution, and both the fault-tolerance and intrusion-tolerance of RHCS outperform other models. However, our study has not taken into account the transformation of backup nodes after node failures. In the future, we will focus on developing a scheduling technique for the backup nodes that will wake up one or more backup nodes when the failure occurs in the network.

APPENDIX

We present major steps in computing the reliability function of the Markov models of section 2.

A. RHCS WITH NO FAULTY NODES

The differential equation of the model is:

$$\begin{cases} P'_{(7,1)}(t) = -(\lambda_{sFT} + 7\lambda_{FT})P_{(7,1)}(t) \\ P'_{(7,0)}(t) = -7\lambda_{FT}P_{(7,0)}(t) + \lambda_{sFT}P_{(7,1)}(t) \\ P'_{(6,1)}(t) = -(\lambda_{sFT} + 6\lambda_{FT})P_{(6,1)}(t) + 7\lambda_{FT}P_{(7,1)}(t) \\ P'_{(5,1)}(t) = -(\lambda_{sFT} + 5\lambda_{FT})P_{(5,1)}(t) + 6\lambda_{FT}P_{(6,1)}(t) \\ P'_{(4,1)}(t) = -(\lambda_{sFT} + 4\lambda_{FT})P_{(4,1)}(t) + 5\lambda_{FT}P_{(5,1)}(t) \\ P'_{(3,1)}(t) = -(\lambda_{sFT} + 3\lambda_{FT})P_{(3,1)}(t) + 4\lambda_{FT}P_{(4,1)}(t) \\ P'_{(2,1)}(t) = -(\lambda_{sFT} + 2\lambda_{FT})P_{(2,1)}(t) + 3\lambda_{FT}P_{(3,1)}(t) \\ P'_{(1,1)}(t) = -(\lambda_{sFT} + \lambda_{FT})P_{(1,1)}(t) + 2\lambda_{FT}P_{(2,1)}(t) \\ P'_{(0,1)}(t) = -\lambda_{sFT}P_{(0,1)}(t) + \lambda_{FT}P_{(1,1)}(t) \\ P'_F(t) = P_F(t) + 7\lambda_{FT}P_{(7,0)}(t) + \lambda_{sFT}(P_{(6,1)}(t) + P_{(5,1)}(t) \\ \qquad +P_{(4,1)}(t) + P_{(3,1)}(t) + P_{(2,1)}(t) + P_{(1,1)}(t) \\ \qquad +P_{(0,1)}(t) \end{cases}$$

Assuming $\lambda_{sFT} = \lambda_{FT}$, and with the initial values $P_{(7,1)}(0) = 1$, $P_{(7,0)}(0) = P_{(6,1)}(0) = P_{(5,1)}(0) = P_{(4,1)}(0) = P_{(3,1)}(0) = P_{(2,1)}(0) = P_{(1,1)}(0) = P_{(0,1)}(0) = 0$, we solve the above equation and obtain:

$$P_F(t) = 1 - e^{-\lambda_{FT}t} - e^{-7\lambda_{FT}t} + e^{-8\lambda_{FT}t}$$

B. MARKOV MODEL OF RHCS WITH STRONG FT NODE FAILURE

The differential equation of the model is:

$$\begin{cases} P'_{(7,0)}(t) = -7\lambda_{FT}P_{(7,0)}(t) \\ P'_{(0,0)}(t) = 7\lambda_{FT}P_{(7,0)}(t) \end{cases}$$

Solving the above equation with the initial conditions $P_{(7,0)}(0) = 1$ and $P_{(0,0)}(0) = 0$ yields:

$$P_F(t) = P_{(0,0)}(t) = 1 - e^{-\lambda_{FT}t}$$

C. MARKOV MODEL OF RHCS WITH STRONG FT NODE FAILURE

The differential equation of the model is:

$$\begin{cases} P'_{(n,1)}(t) = -(\lambda_{sFT} + n\lambda_{FT})P_{(n,1)}(t) \\ P'_{(n-1,1)}(t) = -(\lambda_{sFT} + (n-1)\lambda_{FT})P_{(n-1,1)}(t) \\ \qquad +n\lambda_{FT}P_{(n,1)}(t) \\ \cdots \\ P'_{(1,1)}(t) = -(\lambda_{sFT} + \lambda_{FT})P_{(1,1)}(t) + 2\lambda_{FT}P_{(2,1)}(t) \\ P'_{(0,1)}(t) = -\lambda_{sFT}P_{(0,1)}(t) + \lambda_{FT}P_{(1,1)}(t) \\ P'_F(t) = P_F(t) + \lambda_{sFT}(P_{(n,1)}(t) + P_{(n-1,1)}(t) \\ \qquad + \cdots +P_{(1,1)}(t) \\ \qquad +P_{(0,1)}(t) + P_{(1,1)}(t) + P_{(0,1)}(t)) \end{cases}$$

Assuming $\lambda_{sFT} = \lambda_{FT}$, and with the initial values $P_{(n,1)}(0) = 1$, $P_{((n-1),0)}(0) = \ldots = P_{(1,1)}(0) = P_{(0,1)}\ (0)$

= 0, we solve the above equation and obtain:

$$P_F(t) = 1 - e^{-\lambda_{FT} t}$$

REFERENCES

[1] S. Anand and M. R. K. Keetha, "FPGA implementation of artificial neural network for forest fire detection in wireless sensor network," in *Proc. 2nd Int. Conf. Comput. Commun. Technol. (ICCCT)*, Apr. 2017, pp. 265–270.

[2] S. Deepa, "Energy conservative data transmission using Z-MAC technique in wireless sensor network for environmental monitoring," in *Proc. Int. Conf. Technol. Innov. Agricult. Rural (TIAR)*, Jul. 2016, pp. 194–199.

[3] T. Azzabi, H. Farhat, and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," in *Proc. Int. M&N*, Oct. 2013, pp. 68–73.

[4] G. Scarpato, T. Caputo, A. Caputo, W. De Cesare, A. M. Esposito, and M. Vadursi, "A wireless network as support to the monitoring of Campi Flegrei volcano in Italy," in *Proc. IEEE Int. Workshop Meas. Netw.*, Oct. 2013, pp. 68–73.

[5] R. Lara, D. Benítez, A. Caamaño, M. Zennaro, and J. L. Rojo-Álvarez, "On real-time performance evaluation of volcano-monitoring systems with wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 6, pp. 3514–3523, Jun. 2015.

[6] J. G. Cantuña, D. Bastidas, S. Solórzano, and J.-M. Clairand, "Design and implementation of a Wireless Sensor Network to detect forest fires," in *Proc. 4th. Int. Conf. Ed & Eg (ICEDEG)*, Apr. 2017, pp. 15–21.

[7] S. Abdullah, S. Masar, S. Bertalan, A. Coskun, and I. Kale, "A wireless sensor network for early forest fire detection and monitoring as a decision factor in the context of a complex integrated emergency response system," in *Proc. Int. Conf. Environ. Energy Struct. Monitor. Syst. (EESMS)*, Jul. 2017, pp. 1–5.

[8] M. Younis, S. L. Fatih, and S. Akkaya, "Topology management techniques for tolerating node failure," *Comput. Netw. Int. J. Comput., Telecommun. Netw.*, vol. 58, no. 1, pp. 254–283, Jan. 2014.

[9] T. Wang *et al.*, "Fog-based storage technology to fight with cyber threat," *Future Generat. Comput. Syst.*, vol. 83, pp. 208–218, Jun. 2018.

[10] T. Wang, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and J. Cao, "Big data reduction for a smart city's critical infrastructural health monitoring," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 128–133, Mar. 2018.

[11] S. Petridou, S. Basagiannis, and M. Roumeliotis, "Survivability analysis using probabilistic model checking: A study on wireless sensor networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 4–12, Mar. 2013.

[12] H. Y. Xin and X. X. Liu, "Energy-balanced transmission with accurate distances for strip-based wireless sensor networks," *IEEE Access*, vol. 5, pp. 16193–16204, 2017.

[13] T. Muhammed and R. R. Shaikh, "An analysis of fault detection strategies in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 78, no. 15, pp. 267–287, Nov. 2016.

[14] A. Sargolzaei, C. D. Crane, A. Abbaspour, and S. Noei, "A machine learning approach for fault detection in vehicular cyber-physical systems," in *Proc. 15th Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2017, pp. 636–640.

[15] E. U. Warriach and K. Tei, "Fault detection in wireless sensor networks: A machine learning approach," in *Proc. 16th Int. Conf. Comput. Sci. Eng. (CSE)*, Dec. 2013, pp. 758–765.

[16] S. Zidi, T. Moulahi, and B. Alaya, "Fault detection in wireless sensor networks through SVM classifier," *IEEE Sensors J.*, vol. 18, no. 1, pp. 340–347, Nov. 2017.

[17] S. Rashid, U. Akram, S. Qaisar, S. A. Khan, and E. Felemban, "Wireless sensor network for distributed event detection based on machine learning," in *Proc. Int. Conf. Internet Things (iThings)*, Mar. 2015, pp. 540–545.

[18] C. Titouna, M. Aliouat, and M. Gueroui, "FDS: Fault detection scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 86, no. 2, pp. 549–562, Jan. 2016.

[19] H. Yuan, X. Zhao, and L. Yu, "A distributed Bayesian algorithm for data fault detection in wireless sensor networks," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Mar. 2015, pp. 63–68.

[20] S. Trab, B. Boussaid, A. Zouinkhi, and M. N. Abdelkrim, "Energy minimization algorithm based on Bayesian approach for fault tolerant detection in wireless sensor network," in *Proc. 14th Int. Conf. Sci. Techn. Autom. Control Comput. Eng.*, Apr. 2014, pp. 237–242.

[21] X. Liu, "A survey on clustering routing protocols in wireless sensor networks," *Sensors*, vol. 12, no. 8, pp. 11113–11153, 2012.

[22] N. Jabeur, A. N. S. Moh, and M. M. Barkia, "A bully approach for competitive redundancy in heterogeneous wireless sensor network," *Procedia Comput. Sci.*, vol. 83, no. 10, pp. 628–635, Dec. 2016.

[23] D. G. Costa, F. Vasques, and P. Portugal, "Enhancing the availability of wireless visual sensor networks: Selecting redundant nodes in networks with occlusion," *Appl. Math. Model.*, vol. 42, no. 1, pp. 223–243, Feb. 2017.

[24] B. Zebbane, M. Chenait, and N. Badache, "Exploiting node redundancy for maximizing wireless sensor network lifetime," in *Proc. Int. Conf. (IFIP)*, Nov. 2013, pp. 1–3.

[25] I. El Korbi, Y. Ghamri-Doudane, R. Jazi, and L. A. Saidane, "Coverage-connectivity based fault tolerance procedure in wireless sensor networks," in *Proc. 9th Int. Conf. Wireless Commun. Mobile. Comput. (IWCMC)*, Jul. 2013, pp. 1540–1545.

[26] S. Mukhopadhyay, C. Schurgers, D. Panigrahi, and S. Dey, "Model-based techniques for data reliability in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 8, no. 4, pp. 528–543, Apr. 2009.

[27] W. W. Bein, D. Bein, and S. Malladi, "Reliability and fault tolerance of coverage models for sensor networks," *Int. J. Sensor Netw.*, vol. 5, no. 4, pp. 199–209, Jan. 2009.

[28] A. Munir, J. Antoon, and A. Gordon-Ross, "Modeling and analysis of fault detection and fault tolerance in wireless sensor networks," *ACM Trans. Embedded Comput. Syst.*, vol. 14, no. 1, pp. 1–43, Jan. 2015.

[29] M. Xu, Q. Yang, and K. S. Kwak, "Distributed topology control with lifetime extension based on non-cooperative game for wireless sensor networks," *IEEE Sensors J.*, vol. 16, no. 9, pp. 3332–3342, May 2016.

[30] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[31] G. Zheng and Q. Liu, "Scale-free topology evolution for wireless sensor networks," *Comput. Elect. Eng.*, vol. 39, no. 6, pp. 1779–1788, Aug. 2013.

[32] L. Liu, X. Qi, J. Xue, and M. Xie, "A topology construct and control model with small-world and scale-free concepts for heterogeneous sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2014, no. 1, pp. 1–8, Sep. 2014.

[33] X. Fu, Y. Yang, W. Li, and G. Fortino, "Topology upgrading method for energy balance in scale-free wireless sensor networks," in *Proc. Int. Conf. Network. Sens. Control (ICNSC)*, May 2017, pp. 192–197.

[34] H. Liu, R. Yin, B. Liu, and Y. Li, "A scale-free topology model with fault-tolerance and intrusion-tolerance in wireless sensor networks," *Comput. Elect. Eng.*, vol. 56, pp. 533–543, Nov. 2016.

[35] NIST. *Engineering Statistics Handbook: Exponential Distribution*. Accessed: 2011. [Online]. Available: http://www.itl.nist.gov/div898/handbook/apr/section1/apr161.htm

[36] M. R. Ismail, "Exploiting irregular variable node degree in a MIMO system," in *Proc. Int. Conf. Commun. Syst.*, Nov. 2006, pp. 1–5.

[37] R. Mulligan and H. M. Ammari, "Coverage in wireless sensor networks: A survey," *Netw. Protocols Algorithms*, vol. 2, no. 2, pp. 27–53, 2010.

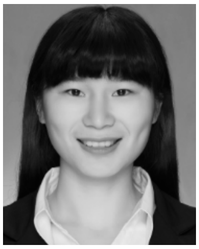
[38] H. H. Zhang and J. C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 1, no. 2, pp. 101–115, Aug. 2005.

[39] K. Mizanian, H. Yousefi, and A. H. Jahangir, "Modeling and evaluating reliable real-time degree in multi-hop wireless sensor networks," in *Proc. Int. Conf. Sarnoff Symp.*, Apr. 2009, pp. 568–573.

[40] A.-L. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," *Physica A, Stat. Mech., Appl.*, vol. 272, no. 1, pp. 173–187, Jul. 2000.

[41] N. Meghanathan, "An algorithm to determine energy-aware maximal leaf nodes data gathering tree for wireless sensor networks," *Comput. Sci.*, vol. 15, no. 2, pp. 96–107, May 2010.

[42] J. Jiang, X. Jin, Y. Xia, B. Ouyang, D. Wu, and X. Chen, "A scale-free topology construction model for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2014, no. 3, pp. 505–521, Aug. 2014.



SHIHONG HU received the bachelor's degree in communication engineering from Jiangnan University, Wuxi, China, in 2016. She is currently a Doctoral Fellow with the School of Internet of Things Engineering, Jiangnan University. Her current research interests include the fault-tolerance of wireless sensor network.

GUANGHUI LI received the M.S. degree from Xiangtan University, Xiangtan, China, in 1999, and the Ph.D. degree from the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China, in 2005, respectively. He was a Professor with the School of Information Engineering, Zhejiang Agriculture and Forestry University, Hangzhou, China. He is currently a Professor with the Department of Computer Science, Jiangnan University, Wuxi, China. He has published over 70 papers in journal or conferences. His research interests include wireless sensor networks, fault tolerant computing, and nondestructive testing and evaluation. His research was supported by the National Foundation of China, Zhejiang, Jiangsu Provincial Science and Technology Foundation, and other governmental industrial agencies.