IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 5, 2020, accepted February 18, 2020, date of publication March 2, 2020, date of current version March 12, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2977759*

# Fault Tolerance Mechanism Combining Static Backup and Dynamic Timing Monitoring for Cluster Heads

**YINGHUA TONG**[1], **LIQIN TIAN**[1,2], **LIANHAI LIN**[1], **AND ZHIGANG WANG**[1]

[1] School of Computer Science, Qinghai Normal University, Xining 810008, China
[2] School of Computer Science, North China Institute of Science and Technology, Beijing 065201, China

Corresponding author: Liqin Tian (tianliqin@ncist.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61862055 and Grant 61762075, in part by the Hebei Provincial Key Research Project under Grant 19270318D, in part by the Hebei IoT Monitoring Engineering Technology Research Center under Grant 3142018055, in part by the National Key Research Project under Grant 2018YFC0808306, in part by the Ministry of Education ''Spring'' Cooperation Project under Grant Z2016083 and Grant Z2016109, in part by the Qinghai Provincial Key Research Project under Grant 2017-ZJ-752, and in part by the Qinghai Key Lab of IoT under Grant 2020-ZJ-Y16.

**ABSTRACT** Internet of things (IoT) monitoring systems have been extensively applied in smart homes, underwater monitoring, volcano monitoring, and health monitoring. In IoT applications, a wireless sensor network (WSN) is deployed to collect data. Hierarchical routing protocols that effectively maintain the energy consumed by sensor nodes (SNs) are usually employed in WSNs. Cluster heads (CHs) are important in this type of protocol. An effective fault tolerance mechanism for CHs in this system can guarantee reliable data acquisition. In this paper, a fault tolerance mechanism that combines CH static backup and dynamic timing monitoring (SBDTM) is proposed, a CH reliability model based on the Markov model is developed, and the minimum number of CHs necessary to satisfy the given reliability requirement is obtained. The data structures and fault-tolerant operations are described, and the energy consumption and the latency of the recovery of the SBDTM mechanism are quantitatively analysed. Simulations were carried out to compare the total network energy consumption, number of dead nodes, throughput, and packet loss rate of the proposed model with those of other methods presented in the literature. The simulation results show that the proposed SBDTM fault tolerance mechanism is superior to current models. This study presents important theoretical and application-based knowledge that can guarantee reliable data acquisition for IoT-based monitoring systems.

**INDEX TERMS** Cluster head failure, fault tolerance, Internet of Things, Markov model, reliability.

## I. INTRODUCTION

Internet of things (IoT) monitoring systems have been extensively applied in smart homes, underwater monitoring, volcano monitoring, and health monitoring. In an IoT monitoring system, data are acquired by a wireless sensor network (WSN) to facilitate the specific applications of the IoT system [1], [2]. WSNs are deployed in wild, harsh environments, where weather and human factors can cause node failure. In addition, because of volume and cost considerations, the nodes in WSNs mostly consist of miniature sensor nodes (SNs) and are generally powered by batteries, which are prone to failure. Hierarchical routing protocols are usually employed in WSNs to reduce node energy consumption [3]. In this type of protocol, if a cluster head (CH) fails, the data collected by the SNs cannot be passed to the sink node. A CH fault can cause the loss of data from all of the SNs in the cluster and the subsequent failure of the IoT monitoring system to obtain the necessary data.

A faulty CH can be replaced by a new CH to ensure normal system operation, albeit by interrupting normal operation. A relatively complex CH re-election scheme can increase the network energy consumption and latency of the recovery of the data transmission; such an increase seriously affects the performance of the system and does not satisfy energy-saving and real-time operation requirements.

Fault tolerance is the ability of a system to immediately and automatically detect and recover from faults [4].

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

Fault tolerance is critical for reliable data delivery in an IoT monitoring system and ensures that the system is available for use during interruptions of any kind or in the presence of faults.

To ensure reliability in an IoT monitoring system, the design of an effective fault tolerance mechanism for CHs is very important. Fault tolerance mechanisms are usually divided into three categories: redundancy-based mechanisms, deployment-based mechanisms, and clustering-based mechanisms [5]. Redundancy-based mechanisms include node redundancy, path redundancy, data redundancy, and time redundancy mechanisms; deployment-based mechanisms include mechanisms before deployment (i.e., fault tolerance during the network design phase), mechanisms during deployment (i.e., fault tolerance during network use), and mechanisms after deployment (i.e., topology-controlled networks). Clustering-based mechanisms achieve the fault tolerance of WSNs by using clusters. Many fault tolerance algorithms are based on the low-energy adaptive clustering hierarchy (LEACH) protocol, which has been accordingly optimized. In this paper, an effective fault tolerance mechanism for CHs is designed to ensure the reliability of an IoT monitoring system.

### A. RELATED WORK

Many mechanisms have been proposed to increase the fault tolerance of CHs to ensure reliability, save energy, and prolong the network lifetime. Bansal *et al.* [6] proposed a fault-tolerant election protocol (FTEP) based on a two-level clustering scheme. The election process appoints a CH and a backup node to handle CH failure. After the failed CH has been identified, the backup CH automatically assumes the CH role. This scheme requires significant power consumption. The use of a single point (backup node) to detect failure can have disastrous consequences. In [7], a fault-tolerant two-level clustering protocol (FTTCP) where each cluster member can separately identify CH failure is presented. Distributed identification is used for every cluster member to reduce power consumption: a CH repeatedly sends a heartbeat message for fault identification. To replace the faulty CH, a backup node is selected as the new CH, and a new backup node is assigned based on the remaining power of the SNs. The simulation results showed that the proposed protocol achieves high fault identification accuracy in a harsh environment and consumes slightly more energy than the FTEP.

Azharuddin *et al.* [8] presented a distributed fault-tolerant clustering algorithm (DFCA) for WSNs to address sudden CH failure. After detecting a CH fault, the member SNs broadcast a HELP message within their communication range. A CH within this communication range can reply to this HELP message, and the SNs join the cluster. Otherwise, an SN within the communication range with the highest residual energy is selected as a relay node to send data to the CH. However, if a faulty CH has many members or there is a simultaneous failure of multiple CHs, the DFCA approach may cause severe HELP messaging problems and inefficient data transmission. Azharuddin *et al.* [9] proposed a distributed fault-tolerant clustering and routing (DFCR) algorithm for energy conservation and fault tolerance in a WSN. The algorithm presented a distributed recovery of the fault cluster members due to sudden failure of the CHs. Kaur and Garg [10] developed an improved distributed fault-tolerant clustering algorithm (IDFCA), which reduces energy consumption by using hierarchy formation to select the CH and replace the faulty node. This scheme can prolong the network lifetime.

To address CH failure, two fault tolerance mechanisms have been proposed: new cluster head generation (NCHG) to elect a new CH and joining the existing cluster head with the best transmission capability (JECHBTC) to join a neighbouring CH. The performances of these two proposed mechanisms were compared with those of the commonly distributed fault tolerance and randomly added backup CH mechanisms [2]. In [11], a CH fault tolerance mechanism that involves a list of backup CHs was proposed. In this mechanism, by taking the sum of the remaining node energies, node degree, and distance between a node and its neighbouring node as the input of a fuzzy inference system (FIS), the opportunity value of a node to become a CH is generated. According to the opportunity value, a list of backup CHs is formed to ensure data transfer between the member nodes and the CHs. In [12], self-configurable cluster head selection (SCCH), a fault tolerance mechanism that combines determination and backup was proposed for CHs. First, at the data transmission stage, if the cluster member nodes do not receive a data request message sent by a CH twice consecutively, then the failing CHs are determined. Second, the member nodes in the backup CH list are employed to promptly replace the failing CHs. This mechanism enhances energy efficiency while prolonging the network lifetime and reducing overhead.

The fault tolerance function of a sink node is achieved by a combination of election and monitoring [13]. When the energy of the sink node falls below a threshold value, a new sink node is elected to replace the original sink node. Reliable operation of the new sink node is achieved as the replaced sink node periodically monitors the remaining energy of the new sink node and backs up the data acquired by the new sink node. This fault tolerance scheme reduces the loss of collected source packets and time without a sink. Gupta *et al.* [14] proposed a fault-tolerant clustering approach based on an inter-cluster monitoring mechanism. This method achieves fault tolerance by regularly checking the gateway state. SNs managed by a faulty gateway are recovered by re-associating them to other clusters based on the backup information created during the time of clustering. A cluster-member-based fault-tolerant mechanism (CMATO) [15] uses the SNs' listening capabilities to monitor CH activity. In CMATOs, cluster members are responsible for detecting faulty CHs by monitoring their links to the CH. The simulation results showed that the proposed protocol performed better in terms of fault coverage and energy consumption. Khan *et al.* [16] proposed a zone-based fault-tolerant management architecture (ZFTMA) for WSNs. To minimize resource utilization, the network is divided into four regions. Each zone is monitored by the zone manager node (ZM). ZFTMAs implements four levels of fault management, including self-managed CH rotation, SN fault detection, CH node fault detection, and CH fault recovery. Each CH continuously monitors its remaining energy levels. SN failures are detected by the CHs. The ZM detects CH faults and initiates CH fault recovery within its supervised zone. To complete the fault management, the WSN should be monitored and scanned in real time. Node monitoring has a variety of schemes, including active monitoring, passive monitoring, reactive monitoring and proactive monitoring [17]. Alrajei *et al.* [18] proposed techniques to prevent failures in a WSN by monitoring the node status, power levels, link quality, and network congestion. Mitra and Das [19] proposed a fault recovery algorithm, in which recovery actions are based on fault diagnosis notification. The algorithm performs recovery using data checkpoints and state checkpoints of the node in a distributed manner. The topology and connectivity between two nodes are preserved. For rapid recovery, primary-backup replication protocols are extensively applied in different application settings, including distributed databases, web services, and the IoT. Guler and Ozkasap [20] addressed various combinations of checkpoint and primary-backup replication mechanisms to improve the efficiency of these mechanisms, especially in terms of lower blocking times and higher throughput. Ai *et al.* [21] proposed a smart collaborative routing protocol for reliable data diffusion in IoT scenarios. The protocol integrates directed diffusion routing, Greedy Perimeter Stateless Routing, and the inspecting node mechanism. In accordance with game theory, the inspecting node is selected to monitor the network behavior. The scheme performed better in terms of network delay, packet loss ratio, and throughput.

Two localization-free and energy-efficient algorithms have been proposed to bypass the holes formed by group collapse [22]. Holes are modelled using clusters, and hole bypassing is solved by cluster bypassing. Intra-cluster and inter-cluster bypassing are employed to heal corrupted communication links in the presence of holes. These algorithms significantly improve fault recovery percentages while consuming a reasonable amount of energy, even in the presence of a high collapse ratio. In addition, this scheme can be easily integrated into many protocols. Elsayed *et al.* [23] presented a distributed self-healing approach (DSHA) to detect, diagnose, and respond to hardware failures in WSNs; this approach enhances WSN reliability and performance. The proposed mechanism is accomplished in four core phases (an initialization/deployment phase, a computation phase, a fault detection phase, and a fault diagnosis and recovery phase) at two levels: the CH level and the node level. The experimental results showed that DSHA was reasonably efficient in fault detection and diagnosis and improved the network lifetime.

In [24], a cluster-based fault-tolerant technique that involves a genetic algorithm was presented for a WSN. A set of backup nodes is selected for each CH. The key element of this technique is that the genetic algorithm is applied in the union of sponsored coverage of the backup nodes to include the sensing area of the failed node. The parameters of the residual energy, distance, link quality, sponsored coverage, burst loss limit, and fault detection timer were investigated. The simulation results showed that the proposed method minimized the energy and the packet loss with reduced delay. Unbalanced clustering and fault tolerance are considered in the particle swarm optimization-based unequal and fault-tolerant clustering (PSO-UFC) protocol [25]. To solve the hot spot problem, the proposed protocol considers an additional CH, which is referred to as the secondary cluster head (SCH) for CH nodes. The simulation results showed that the proposed protocol performed better in terms of the network lifetime and total energy consumption.

Evcimen *et al.* [26] extensively evaluated the performance of distributed self-stabilizing dominating set algorithms for WSNs. This study is the first experimental evaluation study of self-stabilizing minimal dominating set (MDS) algorithms applied in the WSN domain. Ozkan *et al.* [27] proposed an energy-efficient, self-stabilizing, and distributed algorithm for maximal independent set construction in WSNs with a self-stabilization proof. The simulation results showed that the proposed algorithm outperformed other algorithms in terms of the move count and energy consumption. The framework presented in [28] has been referred to as ECraft. This framework has increased the fault tolerance capability at the node and communication levels. The three techniques of self, group, and hierarchical detection have been applied simultaneously for fault detection and fault recovery. An energy-efficient fault tolerance (EFT) management framework that increases fault tolerance quality and decreases network energy consumption was introduced for WSNs [29]. This framework can accept any protocol that lacks fault tolerance and become integrated into the management framework as an input. The output of the management framework is exactly the same as the input protocol that has acquired fault tolerance. The weakness of the EFT framework is that a pre-copy mechanism is not employed in the recovery phase of the CH nodes. Hu and Li [30] investigated fault tolerance in WSN applications by constructing a regular hexagonal-based clustering scheme (RHCS), analysing the reliability of the scheme, and proposing a scale-free topology evolution mechanism (SFTEM). This scheme improved fault and intrusion tolerance. Jassbi *et al.* [31] proposed a fault tolerance and energy-efficient clustering (FTEC) algorithm to detect and recover the faults of CHs and cluster member nodes by selecting a node as a backup CH. A weighted median is employed to detect and recover the faults of the cluster nodes. To recover a fault, the faulty node is isolated and replaced by a neighbouring node, which is switched from sleep mode to wake-up mode. This scheme improves energy consumption and fault tolerance. Many proposed approaches involve the use of backup CHs (BCHs) [32], [33]. However, a maximum of two BCHs has been considered in the corresponding protocols.

### B. CONTRIBUTIONS

Many research works have provided insights into the fault tolerance mechanisms of CHs, especially when an application is run in wild, harsh environments. Most of these mechanisms tend to use a maximum of two BCHs; consequently, the formation of a cluster is not ensured. Some studies have focused on joining the neighbouring CH; doing so may cause the explosion of a HELP message and the low efficiency of data transmission. Other studies have focused on the CH reselection mechanism, which interrupts the normal operation of a system and increases network energy consumption. Only a few studies have provided a monitoring/checkpoint mechanism to reduce the loss of collected source packets and recovery time. To best of our knowledge, there are no reports on fault tolerance mechanisms that combine backup and monitoring. To reduce energy consumption and the latency of the recovery, we propose a fault tolerance mechanism that combines CH static backup and dynamic timing monitoring. The main contributions of this paper are as follows:

1) Considering that end users have different CH reliability requirements for different IoT monitoring systems, a CH reliability model is constructed based on the Markov model. The number of CHs necessary to meet the reliability requirement can be determined.
2) To avoid network function failure and reduce the energy consumption of fault recovery, static backup of CHs is proposed in the CH selection stage. One of the CHs is selected as the primary CH, and the remaining CHs are designated as backup CH nodes. The backup CH nodes are selected based on energy and distance.
3) Monitoring is important to detect abnormal behaviour in the network. To detect a fault in the primary CH and quickly recover from a transient fault, dynamic timing monitoring is included in the data transmission. The backup CHs successively send data packets at specified time intervals to monitor whether the primary CH is working properly.
4) The analytical and simulation results demonstrate the superiority of the proposed fault tolerance mechanism over current models.

The remainder of this paper is organized as follows: In section II, the construction of the system model is described. In section III, the novel fault tolerance mechanism is presented, and a reliability model for CHs is constructed based on the Markov model. The model performance is analysed in section IV. A performance evaluation is presented in section V. The study is concluded in section VI.

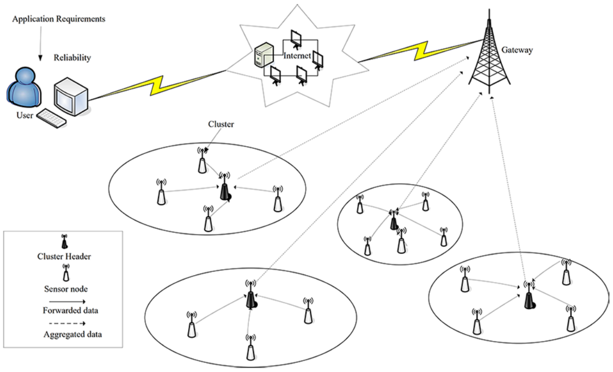

FIGURE 1. Hierarchical sensor network model.

## II. SYSTEM MODEL

### A. NETWORK MODEL

For simplicity, the following assumptions are used in the proposed network model.

The sensor network has a hierarchical structure with a simple path selection: a node does not need to store much routing information. In the hierarchical model, the network is divided into several smaller clusters for management. Each cluster has one CH [34], [35]. The CH collects data from the SNs in the same cluster, performs the necessary fusion processing of the data, and sends the data to the sink node. The sensor (ordinary) nodes continuously collect and transmit sensor data to the CH. Fig. 1 shows the hierarchical sensor network.

1) A few nodes are equipped with global positioning system (GPS) devices and therefore have known positions. The positions of the other nodes can be determined by ranging or non-ranging technology. The node coordinates are used to determine the partition of each node in advance.
2) The nodes in the partition can adjust the communication radius to ensure normal communication among the nodes in the partition.

### B. FAULT MODEL

Generally, fault tolerance or reliability refers to the ability of a sensor network to maintain functionality such that node failures do not disrupt system performance [36]. A fault-tolerant or reliable sensor network should be able to carry out its overall task in the presence of node failures [4]. In fault-tolerant systems, unique definitions are used to describe different flaws. We use the following definitions, which are commonly applied in WSNs:

*Definition 1 (Fault):* Any disruption of the system.

*Definition 2 (Error):* The effect of a fault on the data.

*Definition 3 (Failure):* A collapse of the system, such that the desired function cannot be provided.

*Definition 4 (Fault Tolerance):* The ability of a functional unit or system to continue to perform a required function in the presence of faults or errors.

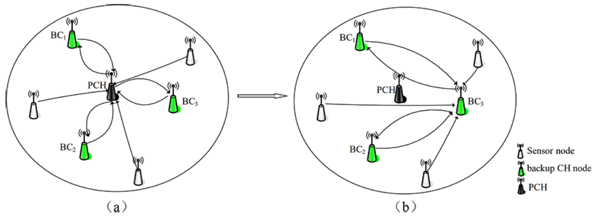

**FIGURE 2.** Schematic of proposed fault tolerance mechanism: (a) Normal PCH and (b) PCH anomalies.

*Definition 5 (Fault Detection):* The detection of faulty functionality in a system by self- or cooperative diagnosis.

*Definition 6 (Fault Recovery):* The recuperation of correct functionality after fault detection by repair or replacement of the failed component.

In our proposed fault model, CH failure is considered to be a software-induced transient fault.

## III. PROPOSED FAULT TOLERANCE MECHANISM AND CH MODEL

### A. PROPOSED FAULT TOLERANCE MECHANISM

To address CH failure, a fault tolerance mechanism that combines the static backup of CH nodes and dynamic timing monitoring (SBDTM) is proposed.

*Definition 7 (Static Backup of CHs):* In the CH selection stage, multiple CHs are successively selected based on the CH reliability requirement of the end user of the IoT monitoring system and a CH selection rule. One of the CHs is selected as the primary CH (PCH) which collects and fuses the data from the SNs. The data are forwarded to the sink node, and the remaining CHs are designated as backup CH nodes.

*Definition 8 (Dynamic Timing Monitoring):* When the data transmission in a cluster is stable, the BCHs successively send data packets at specified time intervals to monitor whether the PCH is working properly. If the PCH is operating normally, the information in the PCH is backed up; otherwise, the backup CH, which currently consists of monitoring nodes, broadcasts the CH advertisement (CH-ADV) to the nodes in the cluster. The backup CH dynamically replaces the failed PCH and becomes responsible for transmitting and receiving data within the cluster.

The proposed SBDTM mechanism for a hierarchical sensor network is shown in Fig. 2.

### B. PROPOSED SBDTM ALGORITHM

In the proposed SBDTM algorithm, the initial dataset of the PCH is Data = { init }, the remaining energy of the PCH is $E_{ch}$, the threshold remaining energy of the PCH set by the user is $E_{th}$, the number of CHs is n, the total number of SN in the cluster is m-1, the dataset of the backup CHs is BCH = $\{BC_1, BC_2, \ldots, BC_j, \ldots, BC_{n-1}\}$, the dataset of the SNs is SN = $\{SN_1, SN_2, \ldots, SN_i, \ldots, SN_{m-1}\}$, and the data collected by the $SN_i$ are represented by $S_i$. The time interval for the backup CH monitoring is equal to that assigned to the SNs by the PCH. The time axis of the different nodes in this mechanism is shown in Fig. 3.

The following pseudo-code in Algorithm 1 shows how the SBDTM algorithm is implemented. With this proposed scheme, the IoT monitoring system can obtain reliable data.

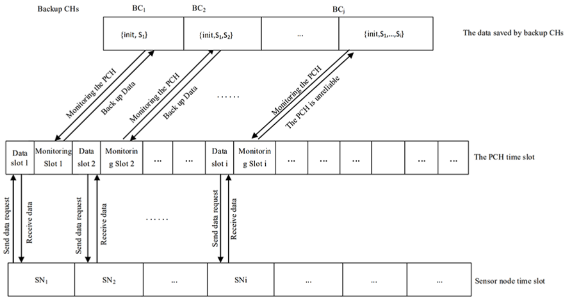

**FIGURE 3.** Timeline of operations in a cluster that performs the fault-tolerant scheme.

**Algorithm 1** Fault Tolerance Algorithm of Our Proposed Scheme

```
Input: $E_{th}$, PCH, BCH, SN, n, m.
Output: Data
Initialize i = 1, j = 1, Data = {init};
Repeat
PCH sends data packets to $SN_i$;
$SN_i$ transmits sensor data to PCH;
$Data = Data \bigcup \{S_i\}$;
Backup $BC_j$ sends data packets to monitor PCH;
PCH sends Ech & Data to backup $BC_j$;
    If ($E_{ch} > E_{th}$) then
            Backup $BC_j$ save Data;
            i = i + 1;
                IF (j < n − 1) then
                    j = j + 1;
                End
                Else
                    j = 1;
                End
    End
    Else
    Backup $BC_j$ broadcasts CH-ADV message to nodes;
    All elements in the SN send a request message to join the cluster;
                IF (j < n − 1) then
                    j = j + 1;
                    End
                Else
                    j = 1;
                End
    End
    Until (i >= m − 1); /*The entire data collection period T ends */
    Return Data;
```

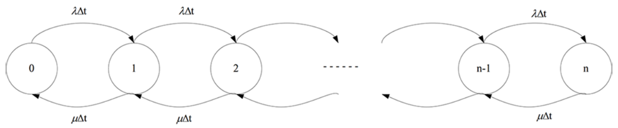

**FIGURE 4.** State transition diagram.

### C. RELIABILITY MODELLING OF CHS BASED ON THE MARKOV MODEL

In different IoT monitoring systems, end users have different CH reliability requirements; therefore, the number of backup CHs varies. When the PCH is normal, the remaining n-1 CHs are backups; when the PCH fails, one of the backup CHs dynamically replaces the failed node and becomes the new PCH. The CH reliability model based on the Markov model is constructed as follows:

1) The switch is completely reliable, and switching is instantaneous.
2) The lifetime distribution of each CH is 1-e$^{-\lambda t}$, t≥ 0(λ: failure rate).
3) A CH fault is a software-induced transient fault.
4) Instantaneous faults can be repaired by restarting the nodes.
5) The repair time distribution after failure is 1-e$^{-\mu t}$, t≥ 0($\mu$: repair rate).
6) All of the random variables are independent.
7) The end user's reliability requirement for the CH is $R_0$.

The constructed CH state transition diagram based on the Markov model is shown in Fig. 4. The Markov process has a state-set $\{0, 1, 2, \ldots, n-1, n\}$, where $0, 1, 2, \ldots, n-1$ are transients; thus, the number of selected static BCHs has $0, 1, 2, \ldots, n-1$ failed states. State n is the absorbing state; thus, all corresponding n CHs have failed and the CHs cannot satisfy the reliability requirement of the system users.

The system has n + 1 different states. We let

$\{X(t) = j\}$; if j faulty parts exist in the system at time t ($j = 1, 2, \ldots, n$),

then

$E = \{0, 1, \ldots, n\}, W = \{0, 1, \ldots, n-1\}, F = \{n\}$

$\{X(t), t \geq 0\}$ is a time-homogeneous Markov process of the state space E.

The state transition diagram (Fig. 4) of the system within $\Delta t$ is used to obtain a transfer rate matrix.

$$A = \begin{pmatrix} -\lambda & \lambda & & & & 0 \\ \mu & -\lambda-\mu & \lambda & & & \\ & \mu & -\lambda-\mu & \lambda & & \\ & & \ddots & \ddots & \ddots & \\ & & & \mu & -\lambda-\mu & \lambda \\ 0 & & & & \mu & -\mu \end{pmatrix} \tag{1}$$

Matrix A is tridiagonal; therefore,

$$\pi_j = (\frac{\lambda}{\mu})^j \frac{\mu^{n+1} - \lambda\mu^n}{\mu^{n+1} - \lambda^{n+1}}, \quad j = 0, 1, \ldots, n \tag{2}$$

Refer to (2),

$$\pi_n = \frac{\lambda^n \mu^{n+1} - \lambda^{n+1}\mu^n}{\mu^{2n+1} - \lambda^{n+1}\mu^n} \tag{3}$$

Because state n is the absorbing state, the reliability of the CH is $R = 1 - \pi_n$.

$$R = \frac{\mu^{n+1} - \lambda^n \mu}{\mu^{n+1} - \lambda^{n+1}} \tag{4}$$

When $R \geq R_0$, the reliability of the CH satisfies the requirement of the end users. When $R = R_0$, parameters λ and $\mu$ are known; therefore, n can be obtained from Equation (4). In this case, the end user reliability requirement is satisfied, and the number of static BCHs is n − 1.

## IV. PERFORMANCE ANALYSIS

In this section, we perform a theoretical analysis of the proposed SBDTM mechanism to show how this mechanism improves NCHG [2] and SCCH [12] in terms of energy consumption and the latency of the recovery.

The SNs in the same cluster are adjacent, and thus, the data from the SNs are spatially correlated [37]. The data packets collected by the CHs have a fixed length. The following assumptions are made:

1) The cluster operation period is T, that is, the time required for each sensor node in the cluster to send the collected data once.
2) Within T, the percentage of CH failures with respect to the total number of transmissions sent by the SNs is P.
3) The latency of the node scheduling is $T_{sdelay}$.
4) The length of the data packet is $L_{pack}$.
5) The energy required for a 1-byte data transmission between two nodes is $E_{tr}$.
6) The energy consumed by the proposed SBDTM mechanism is $E_{SBDTM}$.
7) The energy consumed in the CH reselection mechanism (NCHG) is $E_{NCHG}$.
8) The energy consumed in the SCCH mechanism is $E_{SCCH}$.
9) The latency of the recovery for the proposed SBDTM mechanism is $T_{SBDTM}$.
10) The latency of the recovery for NCHG is $T_{NCHG}$.
11) The latency of the recovery for SCCH is $T_{SCCH}$.

### A. ENERGY CONSUMPTION ANALYSIS

*Theorem 1:* The energy consumption in the proposed SBDTM mechanism ($E_{SBDTM}$) is:

$$[P * (m-1) * (m-2) * L_{pack} * E_{tr} + (1-P) \\ *(m-1) * L_{pack} * E_{tr}] + (m-1) * L_{pack} * E_{tr}$$

*Proof:* Based on the previously stated assumptions, throughout the data collection period T, the number of CH failures is P*(m-1), and the amount of energy consumed ($E_{an}$) is assumed to be:

$$E_{an} = P * (m-1) * (m-2) * L_{pack} * E_{tr} \tag{5}$$

Throughout the data collection period T, the number of normal CH operations is (1-P)*(m-1), and the amount of energy consumed ($E_{nm}$) is assumed to be:

$$E_{nm} = (1-P) \ast (m-1) \ast L_{pack} \ast E_{tr} \tag{6}$$

Therefore, the energy consumed by BCH monitoring ($E_{mt}$) throughout the data collection period T is assumed to be:

$$E_{mt} = E_{an} + E_{nm} \tag{7}$$

Throughout the data collection period T, assuming that (m-1) SNs transmit the sensor data, the energy consumed by the CH in receiving the data ($E_{td}$) is:

$$E_{td} = (m-1) \ast L_{pack} \ast E_{tr} \tag{8}$$

In the proposed SBDTM mechanism, the total energy consumed throughout the data collection period T is the sum of the energies consumed by the BCH monitoring, the SNs in sending the sensor data, and the PCH in receiving the data. Therefore,

$$E_{SBDTM} = E_{mt} + E_{td} \tag{9}$$

$$= [P \ast (m-1) \ast (m-2) \ast L_{pack} \ast E_{tr} + (1-P) \ast (m-1) \ast L_{pack} \ast E_{tr}] + (m-1) \ast L_{pack} \ast E_{tr} \tag{10}$$

*Theorem 2* The amount of energy consumed by CH reselection after CH failure ($E_{NCHG}$) is:

$$P \ast (m-1) \ast [(m-1) \ast (m-2) \ast L_{pack} \ast E_{tr} + 2 \ast (m-2) \ast L_{pack} \ast E_{tr}] + (m-1) \ast L_{pack} \ast E_{tr}$$

*Proof:* In the new CH generation (NCHG) model, when a CH fails and the cluster contains only SNs, the steps for CH reselection are described as follows:

All of the SNs use $R_{mc}$ as the communication radius (to ensure communication among all of the members in the cluster, where $R_{mc}$ is twice the CH communication radius $R_c$, as shown in Fig. 5) to broadcast the CH competition message CH_SEL (which includes the message type, node ID, original CH ID, and remaining energy, where the message type indicates that this message is a CH competition message).

Assume that the broadcast energy consumed by m-1 nodes ($E_{sel}$) is:

$$E_{sel} = (m-1) \ast (m-2) \ast L_{pack} \ast E_{tr} \tag{11}$$

Meanwhile, the node with the highest amount of remaining energy becomes the CH and broadcasts the message CH_SUCC (including the message type and node ID), which indicates successful competition.

The amount of energy consumed by broadcasting a successful competition message ($E_{suc}$) is assumed to be:

$$E_{suc} = (m-2) \ast L_{pack} \ast E_{tr} \tag{12}$$

After receiving the CH_SUCC message, the nodes in the cluster send the message CH_JOIN_REQ (including the message type, node ID, and CH ID) to join the cluster, and the CH sends the message CH_JOIN_SUCC (including the message type, node ID, member ID, and time interval).

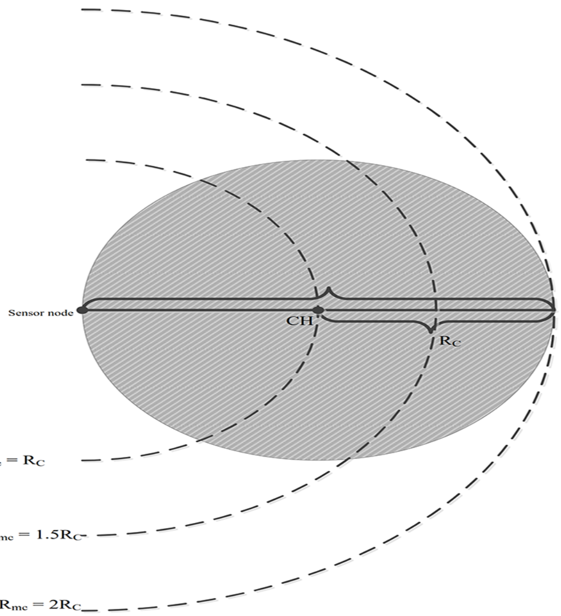

**FIGURE 5. Schematic broadcasting of CH competition message by sensor nodes.**

The energy required for the nodes to become member nodes of a new CH ($E_{meb}$) is assumed to be:

$$E_{meb} = (m-2) \ast L_{pack} \ast E_{tr} \tag{13}$$

Therefore, the energy consumed by one CH reselection ($E_{elect}$) is:

$$E_{elect} = E_{sel} + E_{suc} + E_{meb} \tag{14}$$

The energy consumed by the reselection of the CH during the data collection period ($E_{reelec}$) is:

$$E_{reelec} = P \ast (m-1) \ast [(m-1) \ast (m-2) \ast L_{pack} \ast E_{tr} + 2 \ast (m-2) \ast L_{pack} \ast E_{tr}] \tag{15}$$

The total energy consumption for the CH reselection throughout the data collection period T is the sum of the energies consumed by CH reselection, sensor data transmission by the member nodes, and data receipt by the CHs; therefore,

$$E_{NCHG} = P \ast (m-1) \ast [(m-1) \ast (m-2) \ast L_{pack} \ast E_{tr} + 2 \ast (m-2) \ast L_{pack} \ast E_{tr}] + (m-1) \ast L_{pack} \ast E_{tr} \tag{16}$$

By using the SCCH mechanism, the energy consumption can be obtained in the same way.

$$E_{SCCH} = P \ast (m-1) \ast [3 \ast (m-1) \ast L_{pack} \ast E_{tr}] + (m-1) \ast L_{pack} \ast E_{tr} \tag{17}$$

### B. ANALYSIS OF LATENCY OF RECOVERY

In this paper, a media access control (MAC) protocol based on time division multiple access (TDMA) is adopted.

*Theorem 3:* The latency of the data transmission recovery ($T_{SBDTM}$) in the proposed SBDTM mechanism is:

$$T_{sdelay} + (m-1) * T_{sdelay}$$

*Proof:* In the proposed SBDTM mechanism, the latency required for monitoring the PCH ($T_{mt}$) by the BCHs is:

$$T_{mt} = T_{sdelay} \tag{18}$$

The latency required for broadcasting the CH-ADV message to m-1 SNs after one of the BCHs replaces the PCH ($T_{broad}$) is:

$$T_{broad} = (m-1) * T_{sdelay} \tag{19}$$

Therefore, the latency of the data transmission recovery in this mechanism is:

$$T_{SBDTM} = T_{mt} + T_{broad} = T_{sdelay} + (m-1) * T_{sdelay} \tag{20}$$

*Theorem 4:* In the NCHG model, the latency of the data transmission recovery ($T_{NCHG}$) is:

$$[2*(m-2)+(m-1)*(m-2)]*T_{sdelay}$$

*Proof:* For the NCHG model [2], the latency required for the broadcasting of the CH competition message CH_SEL by all SNs using $R_{mc}$ as the communication radius ($T_{sel}$) is assumed to be:

$$T_{sel} = (m-1)*(m-2)*T_{sdelay} \tag{21}$$

The latency required for broadcasting a successful competition message CH_SUCC when the node with the most remaining energy becomes the CH ($T_{suc}$) is assumed to be:

$$T_{suc} = (m-2)*T_{sdelay} \tag{22}$$

The latency required for all member nodes to send the request message CH_JOIN_REQ after receiving the CH_SUCC message ($T_{meb}$) is assumed to be:

$$T_{meb} = (m-2)*T_{sdelay} \tag{23}$$

Therefore, the latency of the data transmission recovery ($T_{NCHG}$) from CH reselection is:

$$\begin{aligned} T_{NCHG} &= T_{sel} + T_{suc} + T_{meb} \\ &= [2*(m-2)+(m-1)*(m-2)]*T_{sdelay} \end{aligned} \tag{24}$$

By using the SCCH mechanism, the latency of the data transmission recovery can be obtained in the same way.

$$T_{SCCH} = 2*(m-1)*T_{sdelay} \tag{25}$$

## V. PERFORMANCE EVALUATION

In this section, we present the evaluation results for the SBDTM mechanism. We compare the performance indices from the analytical and simulation results. We evaluate the proposed scheme in terms of energy consumption, the recovery latency, the number of dead nodes, the throughput, and the packet loss rate.

**TABLE 1. Simulation parameters.**

| Parameter | Value |
|---|---|
| Number of nodes | 100 |
| Area | 200 × 200 |
| BS position | (100,100) |
| Initial energy (J) | 0.75 |
| $E_{elec}$ | 50 nJ/bit |
| $\varepsilon_{fs}$ | 100 $PJ/bit/m^2$ |
| MAC | 802.15.4 |
| Radio range (m) | 100 |
| $\lambda$ | $1 \times 10^{-4}$ |
| $\mu$ | $2 \times 10^{-4}$ |
| Broadcast message size | 32 bits |
| Monitory message size | 16 bits |

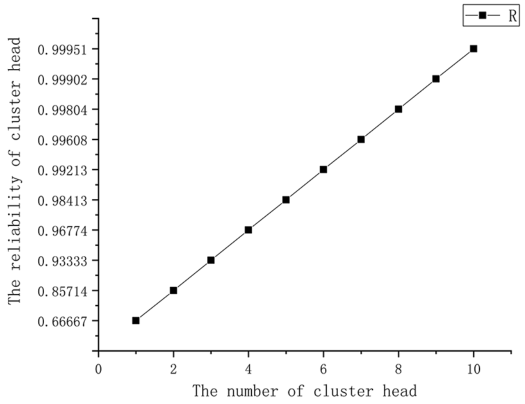

**FIGURE 6.** Relationship between reliability and the number of CHs.

### A. SIMULATION ENVIRONMENT

SBDTM, NCHG and LEACH are implemented on the NS3 simulator in C++ language to compare the performance of these mechanisms. The simulation environment is described in this section. The WSN has 100 nodes, which are randomly deployed and distributed over a square area of 200 m * 200 m. Each SN is assumed to have an initial energy of 0.75 J. The base station (BS) is located at (100,100). The network parameters are shown in table 1.

### B. RELIABILITY OF CHS

Equation (4) demonstrates that CH reliability depends on the number of CHs n, the failure rate λ and the repair rate $\mu$. The failure rate λ is set to $1 \times 10^{-4}$, and the repair rate $\mu$ is set to $2 \times 10^{-4}$. To elucidate the relationship between CH reliability and n, a corresponding graph is shown in Fig. 6.

Fig. 6 shows that CH reliability increases as the number of CHs increases. The number of CHs is determined according to the given CH reliability requirement. A cluster CH reliability requirement of 0.8 requires two CHs, whereas a cluster CH reliability requirement of 0.9 requires three CHs. However, the increase in CH reliability with more than four CHs is not distinct.

### C. COMPARISON OF CLUSTER ENERGY CONSUMPTION OF DIFFERENT FAULT TOLERANCE MECHANISMS

In the following experiments, we compare the energy consumption of three fault tolerance mechanisms for CHs.

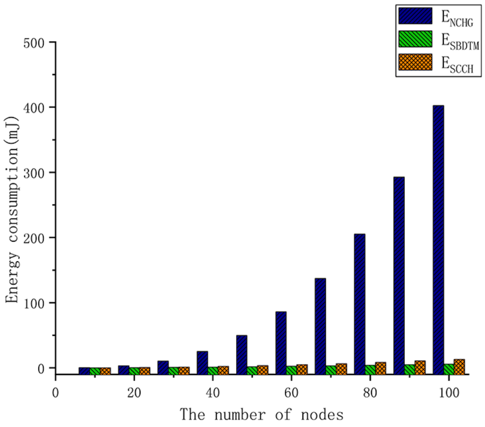

**FIGURE 7.** Total energy consumption of all cluster nodes as a function of the number of nodes.

**TABLE 2.** Total energy consumption over the data collection period.

| Number of nodes | NCHG | SCCH | SBDTM |
|---|---|---|---|
| 20 | 3.14 mJ | 0.64 mJ | 0.52 mJ |
| 40 | 25.29 mJ | 2.27 mJ | 1.39 mJ |
| 60 | 86.10 mJ | 4.88 mJ | 2.59 mJ |
| 80 | 205.25 mJ | 8.48 mJ | 4.11 mJ |
| 100 | 402.38 mJ | 13.06 mJ | 5.96 mJ |

According to Theorems 1 and 2, the total energy consumed by the cluster throughout the data collection period T is related to the number of nodes in the cluster m, length of the data packet $L_{pack}$, percentage of CH failures with respect to the total number of transmissions sent by the SNs P, and energy required for a 1-byte data transmission between two nodes $E_{tr}$. $L_{pack}$ is set to 128 bytes. P is set to 0.04. $E_{tr}$ is set to 80 nJ/byte.

### 1) TOTAL ENERGY CONSUMED BY ALL CLUSTER NODES

We consider the proposed SBDTM, NCHG, and SCCH models throughout the data collection period T for the m values of 20, 40, 60, 80, and 100. We compare the total energy consumption of all of the nodes in the cluster throughout the data collection period T for the three mechanisms. The results are shown in Fig. 7.

The results in Fig. 7 show that for the same number of nodes in the cluster, NCHG consumes more energy than the other two mechanisms. The energy consumed by NCHG sharply increases as the number of nodes increases, while the energy consumed by the proposed SBDTM and SCCH mechanisms increases steadily. The recovery of CH failure in the proposed SBDTM and SCCH mechanisms by the backup CHs reduces energy consumption.

Table 2 shows the total energy consumption over the data collection period.

Table 2 shows that the proposed SBDTM mechanism consumes much less total energy than NCHG. This result confirms our conclusion that the proposed SBDTM mechanism produces more dramatic energy savings than NCHG. In addition, the total energy consumption of the proposed SBDTM mechanism is slightly less than that of SCCH. The proposed SBDTM mechanism combines dynamic timing monitoring to rapidly identify CH failures. However, in SCCH, the SNs continue sending data to the failed CHs, thereby increasing the amount of energy consumption.

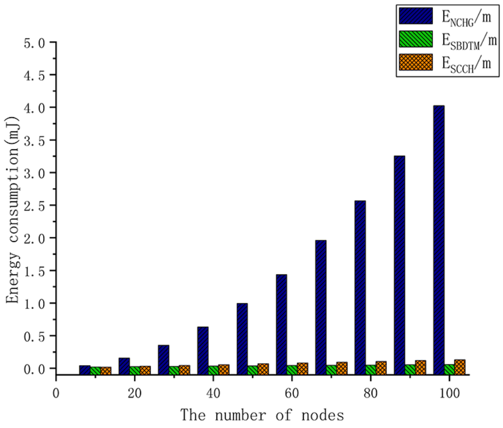

**FIGURE 8.** Average energy consumed by a cluster for different numbers of nodes.

### 2) AVERAGE ENERGY CONSUMED BY A CLUSTER NODE

We consider the m values of 20, 40, 60, 80, and 100 and calculate the average energy consumed by a node in the cluster using the proposed SBDTM, NCHG, and SCCH models.

Fig. 8 shows that for the same number of nodes in the cluster, the average energy consumed by each node is greater when using the NCHG reselection mechanism than when using the other two algorithms. As shown in Fig. 8, the lowest energy consumption per node is obtained using the proposed SBDTM mechanism.

## *D. COMPARISON OF LATENCY OF RECOVERY FOR DIFFERENT FAULT TOLERANCE MECHANISMS*

Equations (20), (24), and (25) show that the latency of recovery depends on m and the latency of scheduling $T_{sdelay}$. $T_{sdelay}$ is set to 20 ms. For the m values of 20, 40, 60, 80, and 100, we compare the latency of recovery for the proposed SBDTM, NCHG, and SCCH models. The results are shown in Fig. 9.

Fig. 9 shows that the longest and shortest latencies of recovery are obtained using NCHG and the proposed SBDTM mechanism, respectively. In the NCHG reselection mechanism, when a CH fails, the SNs in the cluster broadcast the competition message of the CH, thereby increasing the latency of the recovery of the cluster. In SCCH, when an SN does not receive Data-Req, the SN waits until the next frame to receive a request. If the request is not received in the second frame, the CH of the SN is replaced by the BCH. Therefore, SCCH requires a higher latency of recovery than the proposed SBDTM mechanism. The CH failures are quickly identified by the dynamic time monitoring mechanism and handled by the BCHs in the proposed SBDTM mechanism, thereby causing a short latency of recovery.

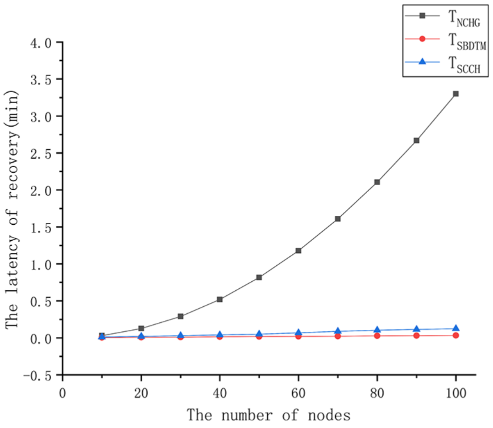

**FIGURE 9.** Relationship between the latency of recovery and the number of nodes.

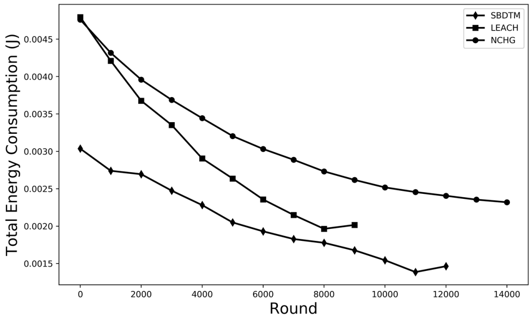

**FIGURE 10.** Total network energy consumption by the network for each round.

The simulation results are shown in the following subsections. For comparative purposes, we ran the fault-tolerant clustering algorithm (LEACH) and NCHG model. We choose LEACH over other competitive clustering methods because it is a simple, fast clustering protocol with minimum clustering overhead.

### E. COMPARISON OF TOTAL NETWORK ENERGY CONSUMPTION

The total network energy consumptions in each round for the different algorithms are compared in Fig. 10.

Fig. 10 shows that SBDTM performs better than LEACH and NCHG in terms of the total network energy consumption. The poor LEACH performance is attributed to CH node selection at the end of each round of the re-clustering stage in a global manner among all of the network nodes, irrespective of whether the CH node fails or not, thereby increasing the amount of energy consumed. For NCHG, when the CH fails, the SNs broadcast the CH competition message over twice the CH communication radius, thereby consuming a massive amount of energy. By contrast, the proposed SBDTM mechanism recovers CH failures using the backup CHs, thereby considerably reducing the amount of energy dissipation.

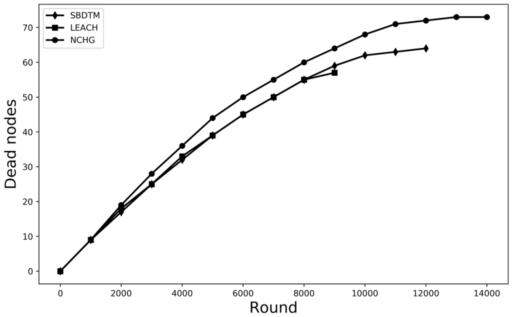

**FIGURE 11.** Number of dead nodes in each round.

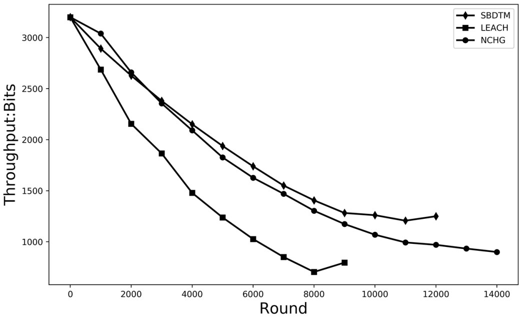

**FIGURE 12.** Throughput for each round.

### F. COMPARISON OF THE NUMBERS OF DEAD NODES

In Fig. 11, the results are compared in terms of the numbers of dead nodes.

Fig. 11 shows that more dead nodes are generated using NCHG than using the other two algorithms, thereby indicating that NCHG is energy-consuming. SBDTM identifies slightly fewer dead nodes than LEACH, although each of these two algorithms produces a comparable number of dead nodes. The reduction in energy consumption of the proposed SBDTM mechanism as a result of the recovery of CH failures by the backup CHs shows that SBDTM has a longer lifetime than NCHG and LEACH. The results also confirm our conclusion that SBDTM reduces energy dissipation.

### G. THROUGHPUT COMPARISON

Fig. 12 shows the throughput in each round; the throughput is calculated as the accumulative size of the unique data that are successfully transmitted to the BS in each round.

Fig. 12 shows that SBDTM has a higher throughput than LEACH, as SBDTM (unlike LEACH) provides BCHs for SNs when PCH faults occur. Thus, more data can be transmitted to the BS in the proposed SBDTM mechanism, thereby increasing the throughput. The throughput of SBDTM is higher than that of NCHG. In NCHG, when CHs fail, the SNs start to reselect new CHs, at which point data are not transmitted to the BS. However, in the proposed SBDTM mechanism, CH failures are quickly identified by the dynamic time monitoring mechanism and recovered by backup CHs;

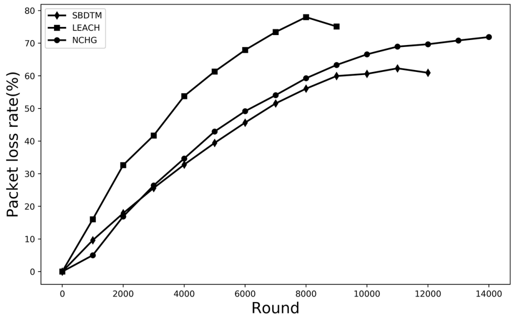

**FIGURE 13.** Packet loss rate for each round.

**TABLE 3.** Complexity comparison of four algorithms.

| | Time Complexity | Space Complexity | Message complexity |
|---|---|---|---|
| SBDTM | O($D_m$) | O($C_m$) | O(C) |
| Intra-cluster bypass | O($D_m$) | O($C_m$) | O($C_m$) |
| Inter-cluster bypass | O(D) | O($C_m$) | O(bk($C_m$+D)) |
| $A_{MIS}$ | O(N) | O($C_m$) | O(N+C) |

thus, the proposed SBDTM provides an alternative path for the SNs while considerably reducing the amount of energy dissipation. Thus, the SNs in SBDTM can work for longer periods, and more data can be acquired and transmitted to the BS.

### H. COMPARISON OF THE PACKET LOSS RATES

Fig. 13 compares the results in terms of the packet loss rate, which is the ratio of the number of bytes that are actually received by the BS to the number of bytes sent without node failure.

Fig. 13 shows that SBDTM and LEACH have the lowest and highest packet loss rate, respectively. This result is attributed to the high energy consumption and number of dead nodes associated with the LEACH mechanism.

### I. COMPLEXITY ANALYSIS

In this subsection, we perform a complexity analysis of the proposed SBDTM mechanism to show how this mechanism improves upon the intra-cluster bypass, inter-cluster bypass [22], and $A_{MIS}$ [27] in terms of time, space, and message complexity.

Table 3 shows the comparison of time, space, and message complexity of four algorithms.

($D_m$ is the maximum cluster diameter, $C_m$ is the maximum node count in a cluster, D is the network's diameter, b is a constant, k is the maximum number of clusters at the same level, N is the number of nodes in the network, and C is the number of clusters in the network).

SBDTM and intra-cluster bypass have the same time and space complexity. SBDTM has better message complexity than the intra-cluster bypass. The inter-cluster bypass and $A_{MIS}$ have relatively worse time and message complexity.

## VI. CONCLUSION

In this study, an SBDTM fault tolerance mechanism that combines CH static backup and dynamic timing monitoring for CHs is proposed to achieve reliable data acquisition and ensure the reliability of an IoT monitoring system. A Markov model-based CH reliability model is established, and the cluster energy consumption and latency of recovery for the proposed SBDTM are quantitatively analysed. The proposed SBDTM mechanism can effectively reduce the total energy consumed by all of the nodes in a cluster, the average energy consumed by each node in the cluster, and the latency of recovery. Several experiments are conducted to precisely evaluate the performance efficiency of the proposed SBDTM. The simulation results show that compared with LEACH and NCHG, SBDTM is reasonably efficient in reducing the total network energy consumption and packet loss rate and increasing the network lifetime and throughput. The proposed scheme provides an important theoretical basis and has application value for reliable data acquisition in an IoT monitoring system. However, the optimal monitoring time interval has not been considered in this study. The monitoring time interval affects the reliability and performance of an IoT monitoring system. In the proposed SBDTM mechanism, to ensure the reliable data acquisition of an IoT monitoring system, the time interval for backup CH monitoring is equivalent to that of the SNs assigned by the PCH. In future studies, we will investigate the optimum time interval for BCH monitoring to achieve reliability and performance optimization.

## REFERENCES

[1] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards Internet of Things," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2017, pp. 1–6.

[2] J.-W. Lin and Y. Wu, "Performance comparisons of fault-tolerant rouging approaches for IoT wireless sensor networks," in *Proc. ICMLC,* New York, NY, USA, 2018, pp. 295–299.

[3] M. M. Afsar and M.-H. Tayarani-N, "Clustering in sensor networks: A literature survey," *J. Netw. Comput. Appl.*, vol. 46, pp. 198–226, Nov. 2014.

[4] M. Afsar, "A comprehensive fault-tolerant framework for wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 17, pp. 3247–3261, Mar. 2015.

[5] G. Kakamanshadi, S. Gupta, and S. Singh, "A survey on fault tolerance techniques in wireless sensor networks," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, NeW Delhi, India, Oct. 2015, pp. 168–173.

[6] N. Bansal, T. P. Sharma, M. Misra, and R. C. Joshi, "FTEP: A fault tolerant election protocol for multi-level clustering in homogeneous wireless sensor networks," in *Proc. 16th IEEE Int. Conf. Netw.*, New Delhi, India, Dec. 2008, pp. 1–6.

[7] A. Kaur and T. Sharma, "FTTCP: Fault tolerant Two-level clustering protocol for WSN," *Int. J. Netw. Secur.*, vol. 1, no. 3, pp. 28–33, Dec. 2010.

[8] M. Azharuddin, P. Kuila, and P. K. Jana, "A distributed fault-tolerant clustering algorithm for wireless sensor networks," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Mysore, India, Aug. 2013, pp. 997–1002.

[9] M. Azharuddin, P. Kuila, and P. K. Jana, "Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks," *Comput. Electr. Eng.*, vol. 41, pp. 177–190, Jan. 2015.

[10] M. Kaur and P. Garg, "Improved distributed fault tolerant clustering algorithm for fault tolerance in WSN," in *Proc. Int. Conf. Micro-Electron. Telecommun. Eng. (ICMETE)*, Ghaziabad, India, Sep. 2016, pp. 197–201.

[11] C. Wang, W. Shen, H. Hu, "Fault Tolerance and Non-uniform Clustering Algorithm for Wireless Sensor Networks Based on Distributed Fuzzy Controller," (in Chinese), *J. Jilin Univ.*, vol. 56, no. 3, pp. 631–638, Mar. 2018.

[12] D. Izadi, J. Abawajy, and S. Ghanavati, "An alternative clustering scheme in WSN," *IEEE Sensors J.*, vol. 15, no. 7, pp. 4148–4155, Jul. 2015.

[13] I. Saleh, A. Agbaria, and M. Eltoweissy, "In-network fault tolerance in networked sensor systems," in *Proc. workshop Dependability Issues Wireless Ad Hoc Netw. Sensor Netw. (DIWANS)*, 2006, pp. 47–54.

[14] G. Gupta and M. Younis, "Fault-tolerant clustering of wireless sensor networks," in *Proc. WCNC*, New Orleans, LA, USA, 2003, pp. 1579–1584.

[15] Y. Lai and H. Chen, "Energy-efficient fault-tolerant mechanism for clustered wireless sensor networks," in *Proc. 16th Int. Conf. Comput. Commun. Netw.*, Honolulu, HI, USA, Aug. 2007, pp. 272–277.

[16] M. Z. Khan, M. Merabti, and B. Askwith, "A fault-tolerant network management architecture for wireless sensor networks," in *Proc. 11th Int. Conf. Annu.*, Liverpool, U.K., Jun. 2010, pp. 1–6.

[17] S. Mitra, A. De Sarkar, and S. Roy, "A review of fault management system in wireless sensor network," in *Proc. Int. Inf. Technol. Conf.*, Pune, India, 2012, pp. 144–148.

[18] N. Alrajei and H. Fu, "A survey on fault tolerance in wireless sensor networks," in *Proc. ASEENCSC*, Indianapolis, IN, USA, 2014, pp. 1–18.

[19] S. Mitra and A. Das, "Distributed fault tolerant architecture for wireless sensor network," *Int. J. Comput. Inf.*, vol. 41, no. 1, pp. 47–58, Jan. 2017.

[20] B. Güler and Ö. Özkasap, "Efficient checkpointing mechanisms for primary-backup replication on the cloud," *Concurrency Comput., Pract. Exper.*, vol. 30, no. 21, p. e4707, Sep. 2018.

[21] Z.-Y. Ai, Y.-T. Zhou, and F. Song, "A smart collaborative routing protocol for reliable data diffusion in IoT scenarios," *Sensors*, vol. 18, no. 6, p. 1926, Jun. 2018.

[22] O. Yilmaz, O. Dagdeviren, and K. Erciyes, "Localization-free and energy-efficient hole bypassing techniques for fault-tolerant sensor networks," *J. Netw. Comput. Appl.*, vol. 40, pp. 164–178, Apr. 2014.

[23] W. M. Elsayed, S. F. Sabbeh, and A. M. Riad, "A distributed fault tolerance mechanism for self-maintenance of clusters in wireless sensor networks," *Arabian J. for Sci. Eng.*, vol. 43, no. 12, pp. 6891–6907, Nov. 2017.

[24] K. Rajeswari and S. Neduncheliyan, "Genetic algorithm based fault tolerant clustering in wireless sensor network," *IET Commun.*, vol. 11, no. 12, pp. 1927–1932, Aug. 2017.

[25] T. Kaur and D. Kumar, "Particle swarm optimization-based unequal and fault tolerant clustering protocol for wireless sensor networks," *IEEE Sensors J.*, vol. 18, no. 11, pp. 4614–4622, Jun. 2018.

[26] H. T. Evcimen, V. K. Akram, and O. Dagdeviren, "Performance evaluation of distributed self-stabilizing dominating set algorithms in wireless sensor networks," in *Proc. 5th Int. Conf. Electr. Electron. Eng. (ICEEE)*, Istanbul, Turkey, May 2018, pp. 428–432.

[27] O. Arapoglu, V. K. Akram, and O. Dagdeviren, "An energy-efficient, self-stabilizing and distributed algorithm for maximal independent set construction in wireless sensor networks," *Comput. Standards Inter.*, vol. 62, pp. 32–42, Feb. 2019.

[28] M. N. Cheraghlou, A. Khadem-Zadeh, and M. Haghparast, "Increasing lifetime and fault tolerance capability in wireless sensor networks by providing a novel management framework," *Wireless Pers. Commun.*, vol. 92, no. 2, pp. 603–622, Aug. 2016.

[29] M. N. Cheraghlou, A. Khadem-Zadeh, and M. Haghparast, "EFT: Novel fault tolerant management framework for wireless sensor networks," *Wireless Pers. Commun.*, vol. 109, no. 2, pp. 981–999, May 2019.

[30] S. Hu and G. Li, "Fault-tolerant clustering topology evolution mechanism of wireless sensor networks," *IEEE Access*, vol. 6, pp. 28085–28096, 2018.

[31] S. Jafarali Jassbi and E. Moridi, "Fault tolerance and energy efficient clustering algorithm in wireless sensor networks: FTEC," *Wireless Pers. Commun.*, vol. 107, no. 1, pp. 373–391, Apr. 2019.

[32] E. Hussain, X. Zhang, L. Chao, and S. A. Bugti, "Fuzzy based smart selection of cluster head with backup support in wireless sensor network," in *Proc. ICCNT*, Coimbatore, India, 2012, pp. 235–239.

[33] D. Izadi, J. Abawajy, and S. Ghanavati, "A new energy efficient cluster-head and backup selection scheme in WSN," in *Proc. IEEE 14th Int. Conf. Inf. Reuse Integr. (IRI)*, San Francisco, CA, USA, Aug. 2013, pp. 408–415.

[34] X. Liu, "A typical hierarchical routing protocols for wireless sensor networks: A review," *IEEE Sens J.*, vol. 15, no. 10, pp. 5372–5383, Oct. 2015.

[35] 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.

[36] S. Chouikhi, I. El Korbi, Y. Ghamri-Doudane, and L. Azouz Saidane, "A survey on fault tolerance in small and large scale wireless sensor networks," *Comput. Commun.*, vol. 69, pp. 22–37, Sep. 2015.

[37] H. Jiang, J. Qian, and J. Zhao, "Cluster head load balanced clustering routing protocol for wireless sensor networks," in *Proc. Int. Conf. Mechatronics Autom.*, Changchun, China, Aug. 2009, pp. 4002–4006.

**YINGHUA TONG** received the M.S. degree from Qinghai Normal University, Xining, China, in 2009, where she is currently pursuing the Ph.D. degree with the School of Computer Science. Her research interests include the fault tolerance of wireless sensor networks and the reliability analysis of the Internet of Things.

**LIQIN TIAN** received the Ph.D. degree in information engineering from the Beijing University of Science and Technology, in 2009. He was a Postdoctoral Researcher with Tsinghua University, from 2009 to 2011. He is currently a Ph.D. Supervisor with Qinghai Normal University and a Professor with the North China Institute of Science and Technology. His research interests include computer networks, performance evaluation, network security, and the Internet of Things.

**LIANHAI LIN** is currently pursuing the M.S. degree with the School of Computer Science, Qinghai Normal University. His research interests include the reliability analysis of the Internet of Things, data mining, and machine learning.

**ZHIGANG WANG** received the M.S. degree from Qinghai Normal University, Xining, China, in 2019, where he is currently pursuing the Ph.D. degree. His research interests include data mining and machine learning.