Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 352062, 10 pages
http://dx.doi.org/10.1155/2013/352062

Research Article

Resilient Multipath Routing Mechanism Based on Clustering with Intrusion Tolerance

Shukui Zhang,[1,2] Hongyan Zuo,[1] Jianxi Fan,[1] and Juncheng Jia[1]

[1] *School of of Computer Science and Technology, Soochow University, Suzhou 215006, China*
[2] *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjin 210093, China*

Correspondence should be addressed to Shukui Zhang; zhangsk2000@163.com

Received 12 July 2013; Accepted 11 September 2013

Academic Editor: Chongsheng Zhang

Wireless sensor networks (WSNs) integrate sensor technology, communication technology and information processing technology; it is a synthetic discipline. WSNs have been applied into almost all walks of life. However, in many special fields, network security is a basic and important factor which we must concern for. This paper introduces the key management scheme after analyzing the security threats of LEACH protocol. At the same time, we adopt several related mechanisms to protect the communication among the sensor nodes and the confidentiality of the data transmission. Also, we use the mixed multipath mechanism among the clusters to improve the security of the network and strengthen the intrusion tolerance.

1. Introduction

The single path in WSNs just created the optimal path which is from the source node to the convergent node to respond timely to the specific mission requirements, which can save space for storage resources, reduce each communication traffic, and simplify algorithm, but the limited bandwidth will lead to the fact that network reliability is poor and fault tolerance is weak, and a node failure could lead to the fact that the whole link is not available, so designing reliable routing protocol is needed to improve the reliability of data transmission [1]. Multi-path routing is that among the source node and the destination node multiple paths are established, which use the primary path for data transmission; if the primary path fails, suboptimal path continuing for delivery will be selected from the backup paths. Disjoint multi-path is the establishment of a number of no convergent node paths among source node and convergent node, while, if the primary path of the way of a node failses, it will cause the entire link paralysis. In order to solve the problems that winding path introduced, this mechanism allows multiple intersecting nodes among the backup paths and the winding path. Each of the nodes on the primary path has a winding path, multiple winding path as an alternate path to constitute the primary path winding multipath. If a node is not available on the primary path, the routing protocol will select automatically the winding path that bypasses the fault nodes to transmit data to the node, so through the multi-path mode the reliability of the data transmission can be improved [2].

Routing protocol influences the performance of the network importantly, which can be divided into flat routing protocol and cluster routing protocol in the network topology view. In flat routing, each sensor node's status is equal and has the same routing function, which can transmit data through other nodes in the middle, so such structure is simple and easy to maintain and has good robustness. But when the number of nodes is large and the network scale is huge, the management and maintenance of routing will consume more energy, scalability relatively will be poor, as a transit node, which will transmit data more times, and energy consumption will be faster, so the structure is only suitable for small and medium-sized network [3].

Directed diffusion protocol [4] is a query-based flat routing protocol, and routing takes periodic updates and maintenance to adapt to changes in network topology. Convergent node sends query tasks, using the flooding way to spread the interested message to all sensor nodes in the monitoring area. In the process of information dissemination, protocol creates

a gradient which reversely transfers data from the source node to the convergent node. Then the convergent node finds the strengthening path which is the earliest path from the source node to the convergent node path and informs the source node. Eventually, the source node transfers the data collected to the convergent node by this route. The algorithm has good scalability, but both the energy consumption and routing overheads are larger.

The sensor node itself has a small size, it is easy to replace the battery, and so on, so that we must first consider is the energy consumption problem. Now clustering topologies controlling the network are commonly used. In order to balance the network node energy consumption, periodically cluster head selection is usually carried out. Clustering routing is suitable for networks which deploy numbers of nodes and have a large scale. LEACH (Low Energy Adaptive Clustering Hierarchy) protocol [5] is an adaptive clustering topology mechanism, which uses periodic execution process, randomly elects cyclic cluster head, and balances energy distribution networks to each sensor node. The agreement introduces a "round" concept, which stages in the establishment of the cluster head. The node generates a random number between 0 and 1, and if this number is less than $T(n)$, the node will become a cluster head and the elected node will message to inform other nodes that it is a cluster head. Other nodes are usually based on their received signal strength to select a member of clusters and send the message notification to add the cluster head in the cluster. After cluster head receives the request which all nodes join it, the cluster head gives them the communication slot allocation. In stable transmission phase, member nodes of the cluster head node receive the broadcast query request, which is monitored area of data collection, and then send data at one hop to the corresponding slot cluster head. After a period of time, cluster head collects data of which all member nodes were the data sent, and fusion finally sends the result to the base station. As in formula (1), random number $T(n)$ is expressed as follows, where p is the head node of all the nodes in the cluster percentage, r is the current round number, $r \bmod (1/p)$ represent elected cluster heads, the G is nonelected cluster heads:

$$T(n) = \begin{cases} \dfrac{p}{1 - p\left(r \bmod (1/p)\right)}, & n \in G, \\ 0, & \text{other.} \end{cases} \quad (1)$$

However, clustering mechanism will have problems such as the uneven distribution of cluster heads, heavy tasks or fast energy consumption issue that makes them stop working soon, affecting the data transmission or even the entire network topology. To solve this problem, a lot of articles used double cluster head algorithm [6] and join assistant cluster head clustering algorithm [7] to a certain extent, reducing the burden of cluster heads and the total energy consumption of the node. This paper summarizes some of the existing clustering algorithms; we propose a new mechanism to enhance the network fault tolerance.

However, WSNs and the rapid development of related technologies have strong practicality, which makes network security vital and relates people to the hot issue. The network is generally used to collect and process the data which is difficult to reach in harsh environments. Most of the sensor nodes are not tamper-resistant or anticapturing ability; once a node is captured, an attacker can get through information from this node to other nodes in the network. It makes the attack nodes send some error message or do not communicate with other nodes, which even leads to communication link failure resulting in great loss of data. Sensor network security risks are often precise because of the bad node deployment area or the communication methods used. Therefore, it should solve the transmission of information confidentiality, integrity, authenticity, and intrusion detection problem, or even if the network is attacked by malicious ones, and how to maintain their basic communication function is very important [8]. In this paper, we proposed a new scheme which is aimed at analyzing security issues which LEACH protocol security causes, and then we combines the inherent characteristics of the network, whose purpose is to reduce the chance in which the data transmission process information is stolen; nodes are posing or malicious nodes tamper with the information; this makes the node in the process of transmitting data even if the encountered attack will also be able to normalize collaboration work to complete basic tasks.

2. Description of the Problem

Cluster head bears most of the LEACH protocol tasks such as data fusion, forwarding, and communication with the base station. Cluster head task is heavy, which makes of fast energy consumption, but also in the data transfer process, it is more vulnerable to malicious attacks and exposure the transmitted information. It leads to poor network security, and thus the node does not complete the task. Here is a summary of LEACH vulnerable to attack in the following three items [9].

(1) Sybil attack: it refers to a single node emerging with multiple identity. In the cluster head election phase, attacker's multiple identities will lead to many nodes are easy to selects as the cluster heads. Elected malicious node controls most of the data node and further damages of the network.

(2) Hello flooding attacks: according to the means which cluster head send the signal strength, member nodes choose to join a cluster. If a malicious attacker has more energy flooding the entire network broadcast a manner notice strength, many nodes will choose to join this cluster where the malicious node exits, then the network will be vulnerable to the impact of these malicious nodes, which even will cause the network to be unavailable.

(3) Selective forwarding attack: such attacks mean that if a malicious node receives a packet, it will not be forwarded directly to the data integrity, but part of it will be lost or tampered before sending, so that the data cannot be accurately inevitably lead to reach the destination, and this is the loss of capture authenticity and integrity of the data.

The trust evaluation mechanism [10] can discover uncooperative nodes in the network, which can be used to reduce

the probability of being attacked, thus improving data integrity, security, and confidentiality. If the node trust value is introduced, it will be removed from the network after being determined in some way after which we can improve the probability of internal network attacks. But often there are many external malicious network attacks, such as theft, tampering and spoofing. How to take measures to simultaneously solve both internal and external attacks is a problem worthy of study. The literature [9] combines cryptography and proposes a secret sharing technology with intrusion tolerance capabilities clustering routing scheme to improve the data transmission network intrusion tolerance capabilities. In order to reduce energy consumption and improve the route network security, the literature [11] introduced a secure boot program and node two-way mechanism evaluation to detect malicious node is directly removed from the network to enhance the security of the entire network.

In order to reduce the burden of cluster head and the energy consumption of nodes, this paper presents a special feature called "Daemon Node (DN)" whose job is head node selection, path creation, and so on. This node can also be called a "backstage node" or "service node" because even if other nodes are in sleep, they have been in working condition, unless their energy is depleted or there is collapse of the entire network, and the node will be extinct. Then we adopted and improved the literature [9, 11] studied the program, and proposed an Intrusion tolerance based on clustering multipath routing mechanism (ICRM), which uses secret sharing between the nodes; in some way the key is split and assigned to the sensor nodes in the network, and cipher text recovery must be carried out with a threshold common trusted node collaboration. Among neighbors, daemon nodes and cluster head is established the pairs of random key introduced evaluation mechanisms. Data transmission between clusters will use hybrid multi-path mode, hoping to improve the data on the network communication traffic and reduce the probability of the node to be captured, thus reducing the possibility of attacks on the entire network.

3. Network Model

n sensor nodes are randomly deployed in a square of side length L of the monitor area A. Intercluster communication distance at least is greater than the distance between the two cluster heads, and the network collected by cluster head set is connected.

Assume that the daemon node has the following properties: (1) not for data acquisition and integration but to receive the base station it sends query request tasks and broadcast to the member nodes; (2) it maintains the energy of each node, location and other information, and real-time update node status information; (3) it makes dynamic perception node in other cases, such as the new node adding or failure of the node exit; (4) among the cluster nodes and other daemon nodes, virtual path in established for data transmission, maintenance established routes; (5) it is used for controlling cluster head work, such as cluster head direction of data transfer. WSNs model [12] is as follows.

(1) Each sensor node for data transmission contains the same initial energy and each of which has a unique ID number.

(2) After the deployment of sensor nodes which cannot move freely, the base station position is fixed in one place outside of the monitoring area, the daemon nodes and the selected cluster heads position is connected and unified tag.

(3) According to the received signal strength to nodes positioned approximate distance to base station, but which do not know the specific location, or there is no GPS function to obtain accurate position information.

In clustering algorithm, the cluster size is a factor to be considered, for ICRM algorithm which is described as follows.

(1) Taking into account the time required to select a cluster head consumption problem, here is the introduction of the cluster head energy factor and in certain conditions randomly selected T_{CH} whose value is less than the threshold. T_{CH} reference LEACH protocol definition is

$$T_{\mathrm{CH}} = \begin{cases} \dfrac{p}{1 - p\left(r \bmod (1/p)\right)} \dfrac{1}{\sqrt{E_{\mathrm{init}}/E_{\mathrm{current}}}}, & n \in G, \\ 0, & \text{other}, \end{cases} \tag{2}$$

where E_{init} is the initial energy which the remaining nodes in addition to the daemon node have and E_{current} is the node's current energy.

(2) The area covered by each cluster radius is fix (R), which is the same size of each cluster. According to literature [13], R derived optimum radius of the cluster is defined as follows:

$$R = 2\sqrt[4]{\frac{2\pi \times S \times E_{\mathrm{DA}}}{27 \times n \times \varepsilon_{\mathrm{pa}}}}, \tag{3}$$

where S is the total area of the monitoring area, E_{DA} is the integration of energy consumption data 1 bit, and $\varepsilon_{\mathrm{pa}}$ is the energy for power amplification.

(3) For a more balanced distribution, the distance between adjacent randomly selected nodes requires more than D; D is defined as

$$D = 2R + \frac{q}{\sqrt{Lk\pi}}, \tag{4}$$

where q is a constant aimed at area A which can be adequately covered and is almost uniformly distributed.

(4) In order to ensure inter-cluster does not cover and all nodes must belong to a cluster, each cluster daemon node using radius fix (R) sends a message, the node which received information is added to the cluster where the daemon nodes is. If a node receives many messages, select the first notification to join and become a member of the cluster nodes, where each member node is only one hop from the cluster head node, and then the daemon node sends a

confirmation message to indicate that the node can join the cluster.

(5) The daemon node obtains the information or each node in the cluster, denoted as E_{res} for the cluster head residual energy, as E_{avg} for the energy average of all the nodes in the cluster. After the node works for some time, if E_{res} is less than E_{avg}, daemon node will reselect again the cluster head which dynamically updated the node with maximum residual energy.

(6) In this paper, the literature [5] uses the same first-order model of wireless communication.

The sender sends l bit data to the distance d of the energy consumption of the receiver which is

$$E_{tx}(l,d) = \begin{cases} l \times E_{\text{elec}} + l \times \varepsilon_{\text{mp}} \times d^4, & d \geq d_0, \\ l \times E_{\text{elec}} + l \times \varepsilon_{\text{fs}} \times d^2, & d < d_0, \end{cases} \quad (5)$$

L bit data received energy consumed is

$$E_{rx}(l) = l \times E_{\text{elec}}, \quad (6)$$

where E_{elec} is the sending or receiving circuit that consumes energy. d_0 is the distance threshold value:

$$d_0 = \frac{\sqrt{\varepsilon_{\text{fs}}}}{\sqrt{\varepsilon_{\text{mp}}}}, \quad (7)$$

where ε_{mp} is a multichannel attenuation model power amplification factor; when sending the distance is greater than or equal to d_0, multiple attenuation model will be used; ε_{fs} is the power amplification coefficient in the free space model; when the transmission distance is less than d_0, the free-space model will be used.

4. ICRM Working Process

Daemon node contains the encryption key K and the hash function $F()$, by which the data processing function is very difficult to launch a value. Outside the area the base station is in the monitoring of a security zone; all the nodes of the network ID and the key pool are loaded onto the base station, but also each daemon node of the cluster storing the key information which nodes in the cluster and nodes in other cluster nodes and maintaining a key ring, which this article assumes that daemon node has more energy and ability.

4.1. Authentication. Each daemon node is managed and maintained in its cluster, real-time monitors of each cluster node, in which the sole is representative of the cluster where the nodes is, so need to be authenticated to the base station. Here BS is the base station, DN is the daemon node, DN_i is the ith ($i = 1, 2, \ldots, m$) node, A $\rightarrow$ B{C} means that A sends the message C to B, and ACK is the identification.

This phase is as detailed below:

(1) DN_i sends status request message REQ to BS:

$$\text{DN}_i \longrightarrow \text{BS}\{i, \text{REQ}\}; \quad (8)$$

(2) after BS received, find DN_i corresponding ID_i (daemon node identifier) which is calculated $F(\text{ID}_i)$ by $F()$, then calculate $V_i = R_i + F(\text{ID}_i)$, which R_i is selected random value according to different daemon node. Then it is cryptographically certified $\text{MAC}_{R_i}(\text{ACK})$ by R_i, finally BS sends a message to DN_i:

$$\text{BS} \longrightarrow \text{DN}_i \left\{V_i, \text{MAC}_{R_i}(\text{ACK})\right\}; \quad (9)$$

(3) after DN_i, receipt of the message, calculate $F(\text{ID}_i)$ by $F()$, draw $R_i = V_i - F(\text{ID}_i)$, and decrypt $\text{MAC}_{R_i}(\text{ACK})$ by R_i to get ACK. Then DN_i is also a randomly generated number, R_i^*, calculated as $V_i^* = R_i^* + F(\text{ID}_i)$, send a message to BS:

$$\text{DN}_i \longrightarrow \text{BS}\left\{V_i^*, \text{MAC}_{R_i^*}(\text{ACK})\right\}; \quad (10)$$

(4) after BS receipt, calculate $R_i^* = V_i^* - F(\text{ID}_i)$, then decrypt whether the ACK by R_i^*, and if so, DN_i authentication is successful, or need to use retransmission mechanism.

4.2. The Key Distribution and Establishment. Daemon nodes communicate with the base station to inform the number and location of the cluster head. Each cluster head CH_i ($i = 1, 2, \ldots, m$) stores allocation key share. Key segmentation process [9] summarized as follows. The base station first use of encryption function ENC and E will be encrypted secret S, $E = \text{ENC}_k(S)$. Reuse some decomposition algorithm divide E into m obtaining $E_1, E_2, \ldots, E_m$, and assign to each cluster head. Then divide the entire key K into m obtaining $K_1, K_2, \ldots, K_m$. Finally put two tuples (E_i, K_i) ($i = 1, 2, \ldots, m$) as key shadow S_i and send to the cluster head CH_i.

To implement a secure connection between the nodes this requires the establishment the key, because of it includes different types of nodes, in order to reduce the degree of interaction between them; this section of different nodes uses different keys. This reference literature [14] is the key distribution of thoughts to solve the clustering model with daemon nodes that is the setup of all kinds of key nodes. Daemon node and base station are stored as preloaded master key, whose mainfunction is to prevent the network attack during initialization which causes information to be stolen, and K_m generate the key pair which will be automatically deleted. This phase is divided into three parts as follows.

The Establishment of a Key among Nodes and Base Stations. Base station and each daemon node according to K_m generate a session key is as follows:

$$\text{PK}(r) = E(K_m, R), \quad (11)$$

where R is random number for a base, with the daemon node's private key K_i ($i = 1, 2, \ldots, m$) encrypted obtaining R_{K_i} and sent to each daemon node. Communication between daemon nodes and base station in order to guarantee the authentication should be deposited in the key.

The Key Establishment between Daemon Nodes and Member Nodes. Member nodes distribute key share with reference

to the above process of cluster heads share the number for $n - 2m$ (where n is all the nodes numbers, $2m$ is the total number of the cluster heads and daemon nodes), and eventually every member node gets a key from the base station and then directly sends its ID and key to daemon node. The daemon nodes after receiving information query their own key ring to find if there is information matching; if so, they will send a confirmation the members of the cluster head ID and control the establishment of the connection among the member nodes. Use the encryption key pair $K_{\mathrm{DN},i}$ daemon nodes and the communication link between the ith ($i = 1, 2, \ldots, n - 2m$) member nodes, cluster heads, and member nodes communication link between key encryptions for $K_{\mathrm{CH},i}$.

The Key Establishment among the Daemon Nodes. According to K_m and $F()$, generate a unique key and key pair, such as daemon node a, ID for a identifier, and L_a as its position information [15], based on the two having the only key K_a as follows:

$$K_a = F_{K_m}\left(\mathrm{ID}_a, L_a\right). \tag{12}$$

Then each daemon node builds key pair with the neighbor daemon nodes in the cluster. Daemon nodes a and b in neighbor cluster, for example, a broadcasts its ID to its neighbor cluster after receipt of b and compares its stored information in the key ring, if there is corresponding information, to establish a connection between two nodes [14]. They set up the shared secret pair K_{ab} as follows:

$$K_{ab} = F_{K_m}\left(\mathrm{ID}_a, L_a, \mathrm{ID}_b, L_b\right). \tag{13}$$

If b did not correspond to a key, each of them will, respectively, send the message which is the request to establish a shared secret pair to the base station, including their ID. With the receipt of base station, assigne key for them and reply from the key pool, after a and b are received using the decryption key K and gain K_{ab}, finally to establish a connection.

Shared key to establish the schematic is shown in Figure 1.

4.3. Measurement of the Node. In order to improve the legitimacy of node identity in communication, we also need to test the credibility of cluster heads and member nodes; in this section by reference to the literature [11] the ideas of nodes for assessment, when their trust value reaches a certain threshold, are allowed to participate in data transfer; otherwise it is considered entrusted node and deleted from the web directly. This phase is divided into two parts as follows.

Cluster Heads to Member Nodes. Each cluster head is set to a value of moderate threshold T ($0 < T < 1$), using formula (14) calculated member nodes reputation value Cread_i ($i = 1, 2, \ldots, n - 2m$):

$$\mathrm{Cread}_i = \frac{\lambda_1 C + \lambda_2 B}{\left(1 - \lambda_1 - \lambda_2\right) S}, \tag{14}$$

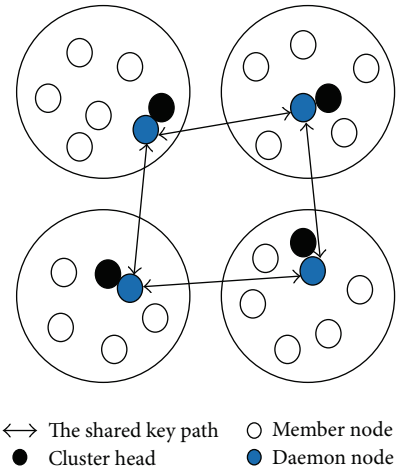

Figure 1: The establishment of a shared secret key.

where C is a member node sending data current, B is the sum of the member nodes to send data before, S is the total number which the member nodes send, λ_1 and λ_2 ($0 < \lambda_1, \lambda_2 < 1$) being both the corresponding weights.

If $\mathrm{Cread}_i \geq T$, members of the node are credible; if $\mathrm{Cread}_i < T$, mark them as malicious nodes.

If member nodes are malicious nodes, after daemon node receives cluster head signal board case, delete the message $\mathrm{mes}_{\mathrm{del}}$. Daemon nodes will store their ID but delete their carrying key. The evaluation mechanism shown in (15) by the way has already been leaked; keys can be deleted from the network, which increase the security of network.

Cluster Head in Member Nodes of the Assessment. Consider

$$\begin{aligned} \mathrm{CM}_i &\longrightarrow \mathrm{CH}\left\{\mathrm{ID}_{\mathrm{CM}_i} \parallel \mathrm{ID}_{\mathrm{CH}} \parallel E\left\{K_{\mathrm{CH},i}, \mathrm{Random}_i, \mathrm{mes}\right\}\right\}, \\ \mathrm{CH} &\longrightarrow \mathrm{CM}_i\left\{\mathrm{ID}_{\mathrm{CM}_i} \parallel \mathrm{ID}_{\mathrm{CH}} \parallel E\left\{K_{\mathrm{CH},i}, \mathrm{Random}_i, \mathrm{mes}_{\mathrm{del}}\right\}\right\}, \end{aligned} \tag{15}$$

where CM_i is the ith member nodes, CH is cluster head, $\mathrm{ID}_{\mathrm{CH}}$ is the cluster identifier, $E\{K\}$ is encryption using the secret key K, Random_i is the ith node which generated random number, and mes is sending information for members of the cluster head.

Member Nodes to Cluster Heads. Evaluation of the above (1) can prevent malicious nodes into the network, but in order to bring more security, it also needs member nodes evaluating cluster head to determine the current cluster heads which can be trusted. This mechanism is shown in the following.

Member Nodes in Cluster Head of the Assessment. Consider

$$\begin{aligned} \mathrm{CM}_i &\longrightarrow \mathrm{DN}\left\{\mathrm{ID}_{\mathrm{CM}_i} \parallel \mathrm{DN} \parallel E\left\{K_{\mathrm{DN},i}, \mathrm{Random}_i, \mathrm{mes}\right\}\right\}, \\ \mathrm{DN} &\longrightarrow \mathrm{CM}_i\left\{\mathrm{ID}_{\mathrm{CM}_i} \parallel \mathrm{DN} \parallel E\left\{K_{\mathrm{DN},i}, \mathrm{Random}_i, \mathrm{mes}_{\mathrm{del}}\right\}\right\}. \end{aligned} \tag{16}$$

What is mentioned above only represents single member nodes in cluster head of assessment; in order to improve the reliability of the results, all the member nodes are involved in the mechanism and then send the result to directly place daemon node in cluster, after daemon nodes received all member nodes in this cluster node test information, and then cluster head judges the credibility.

4.4. Multipath Routing. The literature [16] proposes an improved bulk density of the intrusion-tolerance ability of the routing protocol, to reduce the influence degree of the failure nodes on the network; the experiments show that the new routing protocol can effectively achieve data branching and improving the network capacity intrusion-tolerance ability. But in the literature, a common node in routing is just established, and this section will use the combination of disjoint path and winding path to the multi-path routing established between cluster heads. This phase is in the following three processes.

Build Paths. Because of the time of authentication and key establishing base station already known as daemon node location and distance information, daemon nodes need to send PATHREQ messages (including their own ID) in order to show how to begin the establishment of path. The base station feedbacks the PATHREV information to the daemon nodes after it receives the message, and according to the previously stored information we calculate the distance between them; finally each guard node maintains a routing table.

The Route Choice. First, using Floyd algorithm we calculate the shortest path from source daemon node to the base station and record every daemon node of the path. Then we build short path again, but no longer using the daemon node which is the primary path from source daemon node to base station which it passes by, for example, daemon node A midway through the B and C to base station, when the second shortest path is built; in other daemon node we expect the two nodes again using Floyd algorithm and calculate the second shortest path from A to the base station, as A backup path, and then press the same way to build A next second shortest path to the base station, as the second backup paths, and so on, which constructs the backup paths [17]. Finally using winding path algorithm, we construct the primary and second shortest path winding paths of each daemon node which makes every daemon node in at least one path. Building the multi-path routing diagram is shown in Figure 2.

But this only establishes virtual path among daemon nodes; the daemon node should command and control cluster head communication if daemon nodes and cluster heads position is once established, it will not be changed; even changes in the cluster heads are just changes of the location of the original cluster head and new cluster head. After the success which among cluster heads is the primary path, the second shortest path and winding path are set up and finally step into the stage of data transmission.

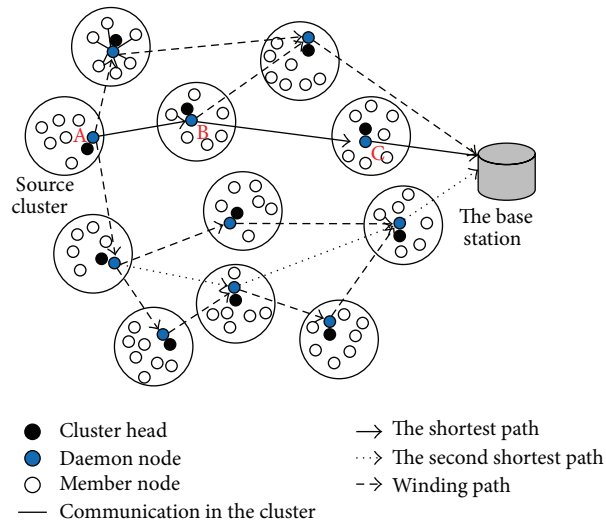

Figure 2: A mix of multi-path.

The Data Transmission Phase. Daemon node preserves the backup in which it and cluster heads have merged data. This section established the shortest path and the second shortest path; member nodes sent the collected information to the cluster heads, primary cluster fusion data and grouped packaging [18–20], a set of data using the shortest path transmission and another group using the second shortest path transmission. The two paths of the next cluster head receive data and fusion of information which it presses and continues to transfer until reaching the base station; base station receive two grouping of the data in the data reorganization, and also needs to get the key information. First we have to collect mS_i of cluster head CH_i ($i = 1, 2, \ldots, m$) on two links, with secret sharing scheme E and the secret key K to recover, finally by using the key K and the DEC decryption E obtaining S, $S = \mathrm{DEC}_K(E)$.

Through the data packet assigned to multiple paths, even if a cluster head is captured within the network, this will not leak the complete information of data. And each cluster head is established by winding path on the primary path; even cluster is attacked, and the data transmission will automatically bypass the failure nodes, and cluster heads will continue information transmission to the base station through the winding path, which can effectively enhance the network capacity invasion ability and improve the efficiency of data transmission.

5. Exception Handling

5.1. The Node Processing. Node failure may be because of its own characteristics or captured, which leads to network topology changes. Daemon nodes have real-timely monitory other nodes, when they find abnormal situation, which will diagnose and do the corresponding processing and store energy of each node information and trust degree, after a period of time if the cluster head energy value is lower than the preset threshold, according to the maintenance of information table selected residually more energy and high

trust value node for the next round of cluster head, cluster head message to broadcast again.

If cluster head is assessed as not credible, the daemon nodes will broadcast cluster head failure message to the member nodes. After the member node is received, it stops sending the collected data to cluster head in the cluster, and daemon nodes will delete the invalid cluster heads and reassign them. If a member node is not credible, daemon node will directly delete that node.

If a new node applies for joining a cluster, it will first send its key to daemon node in the cluster. After daemon nodes receipt, we need to check when a new node is key information and maintain consistent daemon node, the daemon node to perform this node to join operations, but we also need to see cluster head in the evaluation, after assessment can be involved in data collection, transmission, and so forth.

5.2. Routing Maintenance. Multiple paths are to work together, which may be because of a certain path to the cluster head that is attacked or lacks energy, which causes this path fails that then continues and to transmit data through a winding path; the failure path routing maintenance mechanism is adopted to repair in time, elaborated in two different conditions as follows.

(1) If a cluster head in the path fails, daemon nodes automatically sense and from the maintenance of information in the table select the most appropriate member nodes as the cluster head of in the cluster, the source cluster head and the new cluster head exchanged; the new cluster head immediately receives daemon node in the fusion of data backup, established under the control of the daemon nodes into transmission path in waiting for the next round of data transfer.

(2) If this is not suitable for cluster head, the routing failures also show that the cluster heads are unavailable and low energy nodes directly close the communication module of dormancy. Daemon nodes inform base station node, the automatic cluster scatter, the daemon node leaving virtual path; another daemon node is automatically connected to modify maintenance information again.

Using multi-path routing maintenance mechanism, if the path or the cluster heads appear to be problem, they can be restored or replaced in time. If there is not the cluster head which did not meet the conditions, failure of cluster's path directly removed makes some nodes into a dormant state, which can save energy and prolong the service life of them.

6. Performance Evaluation

It puts forward a scheme that is still on the basis of LEACH protocol. The main purpose is to enhance the security of data transmission and improve the reliability of the network; the following is performance of the detailed analysis of the mechanism.

6.1. Process Description. This paper built different keys among the various nodes, and between the two nodes is only key pair. First, the node's join needs verification. The nodes whose validation is not adopted are difficult to enter the network, the node which is successful to join but if the trust value is the lower it will not be able to participate in the transmission of the data. Before communication, each kind of nodes also needs node-to-node authentication, if this succeeded, data transmission can be carried out. Even if a node in the network running process is internal attack, leak is associated with being the attacked node itself, and the content of the other nodes can still work normally. Second, due to the introduction of node evaluation mechanism, cluster head in member node of the assessment can filter out certain malicious nodes, and member nodes of cluster head nodes review will also become a cluster head which has been dropped as a malicious node network, which can be at ease using cluster heads for data fusion and forwarding therefore, to some extent, this mechanism can be resisted. Section 2 summarizes the three kinds of attack.

The establishment of random key pair needs to broadcast each node number, so that we can save the communication traffic. Between source cluster heads and base station the hybrid multi-path mechanism is adopted, concurrent transmission data can be in the path, so that each path will reduce the quantities of data, so as to reduce the path of a single load, which is resolved in a single path on a cluster head energy consumption which is too fast and easily becomes death problem and further can reduce the topology change of path reconstruction or network reconfiguration overhead. In addition, even if building the shortest path, the second shortest path is even more than a certain number of cluster heads as the standby path being attacked, which can also be adopted as timely winding path to transmit data of each cluster head, daemon node using route maintenance mechanism, and the successful replacement of cluster heads to participate in the next round of data transmission, to improve network communication traffic as a whole.

6.2. Evaluation Indicators. This paper compares the ICRM and LEACH; DD agreement, analysis of performance indicators [18] are defined as follows.

Load balancing factor is

$$b_f = \frac{1}{n-m} N_{\text{low}}. \tag{17}$$

This value is used to measure the balance degree of clusters, where N_{low} is the number of energy which is lower than the average of the total number nodes in network, m is the number of daemon nodes, n is the total number of nodes, $n - m$ is the number of participating nodes in the data transmission.

The average end-to-end delay is

$$T_d = \frac{1}{n-m} \sum_{t \in T_s} t_d. \tag{18}$$

It is the average of the sum of the time delays which is transmitted packets from the source cluster heads to the

destination in T_s time, where is the t_d for each participating data transmission delay of cluster heads.

Network throughput is

$$T_p = (n - m)\frac{P_{\text{send}}}{T_s}. \quad (19)$$

It is the number of data packets of successful transmission in T_s time, P_{send} is each cluster head that sends the packet number.

The routing control overhead is

$$E_c = D_c + T_c, \quad (20)$$

where D is the pay expenses which are daemon node controlling according to the built path transmission cluster heads need, T is multiple paths in need of the overhead of data transmission.

6.3. Experimental Verification. Performance in order to verify the proposed algorithm uses c++ programming and corresponding analysis; in this section the ICRM and LEACH and DD protocol defined in the previous section on the evaluation index of were compared, and the running time is a measured parameter. 100 sensor nodes are randomly placed within 100 m × 100 m square area, because nodes are randomly deployed; location is not fixed, and there will be multiple nodes which are stacked in a place where nodes distribution is not uniform, causing no spread to some region; the random node distribution is shown in Figure 3. With base station coordinates of (120, 120), a sensor node range of (0, 0) to (100, 100) area, and node for the initial energy of 1 J, node death occurred when energy is 0, an experiment of assuming no daemon node death.

Figure 4 shows that clustering protocol LEACH in network load balance factor is better than that of flat DD routing protocol, which shows flat routing network load to be better than than clustering routing protocol. ICRM due to daemon node is introduced in the work, in the process of establishing virtual path, cluster head, and member nodes dormancy, in order to reduce energy consumption. In data transmission, the cluster heads packaged data packet transmission in multiple paths, which obviously decrease viral pathways on cluster head load and energy consumption. By comprehensive comparison, this paper presents the mechanism of the minimum balance network load factor and stability.

Figure 5 shows that the flat structure of multi-path routing protocols is used with the DD, compared with LEACH and ICRM clustering mechanism which is significantly smaller average end-to-end delay, which explains clustering structure division of each node clearly and is able to better coordinate the entire network. ICRM generated is the multipath among daemon nodes; cluster heads need to be controlled for data transmission, which is faster than flat routing path of each node speed, whose LEACH from the base station in the remote node increases path establishment and data transmission delay, so the ICRM is average minimum delay here.

Comparison on throughput is shown in Figure 6, because the ICRM introduced invasion mechanism, and it can effectively resist malicious nodes to participate in the network;

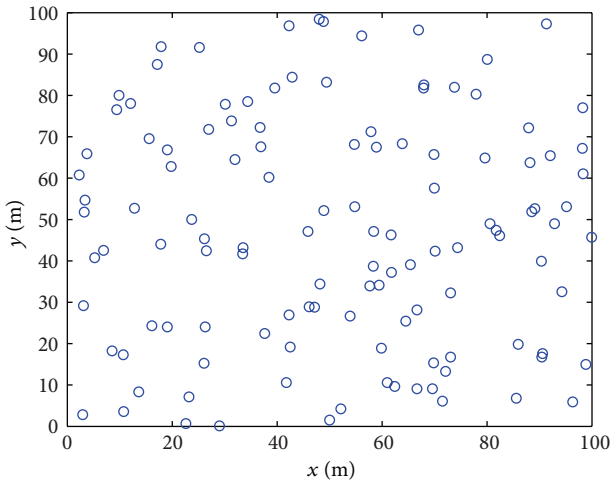

Figure 3: Nodes random distribution.

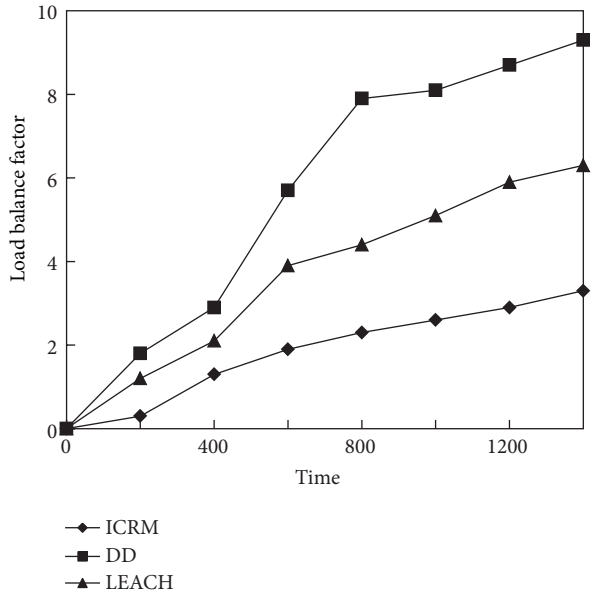

Figure 4: Load balance.

network packets loss rate is smaller, and the cluster head setup between multi-paths makes data transmission more reliable, even if a certain path fails; route maintenance mechanism to take timely measures to make the data transmission is almost unaffected, and routing robustness is better. With daemon nodes splitting the tasks of the cluster head nodes, which can reduce the energy consumption of nodes, each cluster head works longer, with more quantities of data as a whole. While, in DD agreement, most of the nodes energy consumption quickly, easy to death, makes the minimum quantities of data protocol. LEACH protocol cluster head bear there are the mission of the heavier, but member nodes energy consumption less, better than the DD agreement, but uneven distribution of cluster heads, which lead some cluster heads to premature death which affects the data transmission.

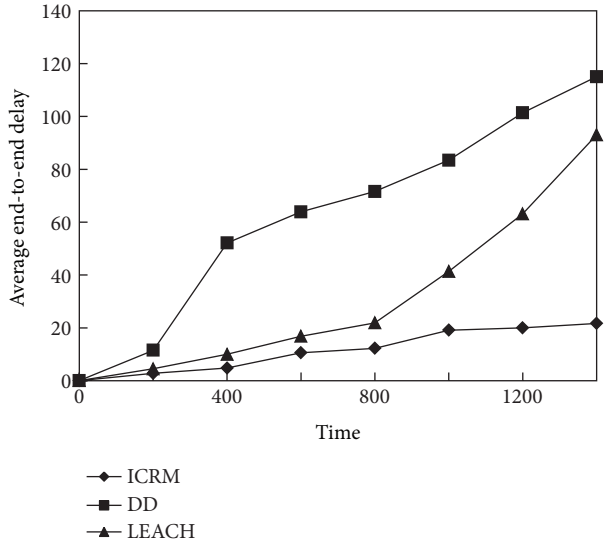

Figure 5: Average end-to-end delay.

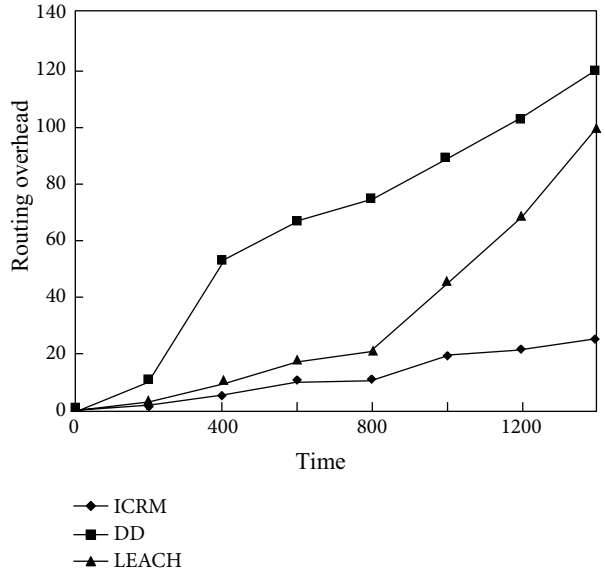

Figure 7: Routing overhead.

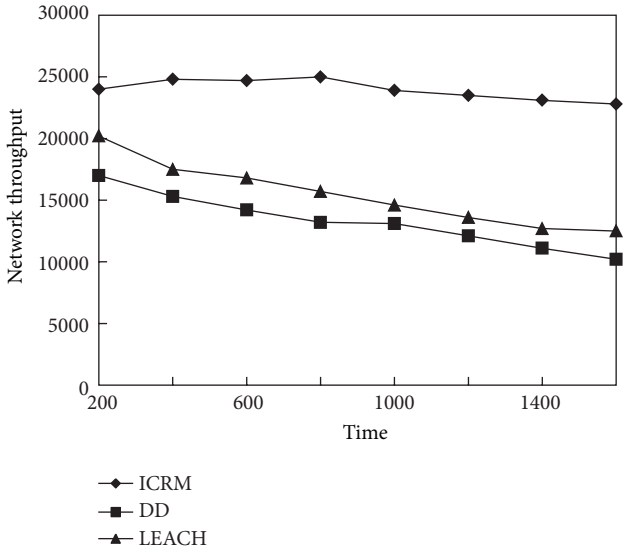

Figure 6: Network throughout.

In Figure 7, because the DD agreement path generation time is long and often interrupted, routing maintenance spends more cost, so the routing control overhead is the largest. Cluster head easy to die in the LEACH protocol and often to be cluster head selection again every time refactoring and controlling the routing overhead are large. ICRM and cluster heads are controlled by daemon node work, and cluster heads are less susceptible to attack and daemon node real-time monitoring work and timely replacement of each failure cluster heads or removal of low trust value of nodes, in each path on the energy balance, almost can be seen from the diagram, the routing mechanism overhead is relatively stable, significantly lower than the other two protocols.

7. Conclusion

This paper to solve the problem was made in the course of the LEACH protocol in data transmission security hidden danger which introduced a simple key management mechanism, the secret sharing technology, and random key to the model of a bunch of key management information into more pieces which were assigned to each sensor node, among daemon nodes, cluster heads, and member nodes which need to be the key of authentication; in a certain moment even network, one or several nodes attack; also will not leak the key information. In order to increase the credibility of the working node we also introduced the node evaluation mechanism, and low trust value node has been dropped as a network cannot be directly involved in data transmission and effectively improve the performance of network security. Data transmission among clusters enhanced multi-path mechanism, which further improves the reliability of data transmission and implements network load balancing.

Acknowledgments

This work is supported by National Natural Science Foundation of China under Grants nos. 61070169, 61201212, Natural Science Foundation of Jiangsu Province under Grant no. BK2011376, Specialized Research Foundation for the Doctoral Program of Higher Education of China no. 20103201110018 and Application Foundation Research of Suzhou of China nos. SYG201118 and SYG201240.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] Z. Bidai, H. Haffaf, and M. Maimour, "Node disjoint multipath routing for ZigBee cluster-tree wireless sensor networks,"

in *Proceedings of the International Conference on Multimedia Computing and Systems (ICMCS '11)*, pp. 1–6, April 2011.

[3] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.

[4] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 174–185, 1999.

[5] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[6] B. V. Nadimpalli, P. Mulukutla, R. Garimella, and M. B. Srinivas, "Energy-aware routing in sensor networks using dual membership clusters and data highways," in *Proceedings of the IEEE Region 10th Conference Analog and Digital Techniques in Electrical Engineering (TENCON '04)*, pp. C184–C187, November 2004.

[7] J. Z. Long, Y. T. Chen, D. M. Deng et al., "Assistant cluster head clustering algorithm based on LEACH protocol," *Computer Engineering*, vol. 37, no. 7, pp. 103–105, 2011.

[8] H. Nabizadeh and M. Abbaspour, "IFRP: an intrusion/fault tolerant routing protocol for increasing resiliency and reliability in wireless sensor networks," in *Proceedings of the International Conference on Selected Topics in Mobile and Wireless Networking (iCOST '11)*, pp. 24–29, October 2011.

[9] H. Yu, J. He, T. Zhang, and P. Xiao, "A group key distribution scheme for wireless sensor networks in the Internet of things scenario," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 813594, 12 pages, 2012.

[10] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 167575, 7 pages, 2013.

[11] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: best practices," *Computer Communications*, vol. 33, no. 9, pp. 1086–1093, 2010.

[12] T. Zhang, L. Li, and C. Yan, "A secure cluster-based router protocol for WSNs," *Chinese Journal of Sensors and Actuators*, vol. 22, no. 11, pp. 1612–1616, 2009.

[13] P. C. Yu, H. Z. Zhang, and Z. J. Liu, "Research of cluster-based multi-hop routing protocol," *Journey of Computer Applications*, vol. 27, no. 2, pp. 351–354, 2007.

[14] M. Liu, J.-N. Cao, G.-H. Chen, L.-J. Chen, X.-M. Wang, and H.-G. Gong, "EADEEG: an energy-aware data gathering protocol for wireless sensor networks," *Journal of Software*, vol. 18, no. 5, pp. 1092–1109, 2007.

[15] P. C. Zhao, Y. Xu, and M. Nan, "A hybrid key management scheme based on clustered wireless sensor networks," in *Proceedings of the IEEE 2nd International Conference on Computer and Management*, pp. 1394–1397, 2012.

[16] X. Sun and E. J. Coyle, "The effects of motion on distributed detection in mobile ad hoc sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 460924, 14 pages, 2012.

[17] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 1, pp. 32–43, 2012.

[18] A. Modirkhazeni, N. Ithnin, and O. Ibrahim, "Secure multipath routing protocols in wireless sensor networks: a security survey analysis," in *Proceedings of the 2nd International Conference on Network Applications, Protocols and Services (NETAPPS '10)*, pp. 228–233, September 2010.

[19] E. Kohno, T. Okazaki, M. Takeuchi, T. Ohta, Y. Kakuda, and M. Aida, "Improvement of assurance including security for wireless sensor networks using dispersed data transmission," *Journal of Computer and System Sciences*, vol. 78, no. 6, pp. 1703–1715, 2012.

[20] C. Chen, W. Wu, and Z. Li, "Multipath routing modeling in ad hoc networks," in *Proceedings of the IEEE International Conference on Communications (ICC '05)*, pp. 2974–2978, May 2005.