**Research Article**

**Improved Reliable Trust-Based and Energy-Efficient Data Aggregation for Wireless Sensor Networks**

Chen-xu Liu, Yun Liu, and Zhen-jiang Zhang

*Key Laboratory of Communication & Information Systems, Beijing Municipal Commission of Education, Beijing Jiaotong University, Beijing 100044, China*

Correspondence should be addressed to Chen-xu Liu; hhtslcx@gmail.com

Received 16 December 2012; Revised 2 May 2013; Accepted 9 May 2013

Academic Editor: J. Barbancho

Copyright © 2013 Chen-xu Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In wireless sensor networks, secure data aggregation is very important for reducing the quantity of data transmitted and prolonging the lifetime of wireless sensor networks. When wireless sensor networks are deployed in untrusted and hostile environments, their nodes are often compromised, which reduces the security and reliability of the transmitted data. Compromised nodes can inject erroneous data, selectively forward data to an adversary, impersonate legal nodes to join routing paths, and disrupt data transmission during the data-aggregation operation. Previous researchers have relied on reputation system to find compromised nodes and prevent attacks during the data-aggregation operation. In this paper, we propose an improved reliable, trust-based, and energy-efficient data-aggregation protocol for wireless sensor networks. We call the protocol the iRTEDA protocol, and it combines the reputation system, residual energy, link availability, and a recovery mechanism to improve secure data aggregation and ensure that the network is secure, reliable, and energy-efficient. Simulations have shown that the iRTEDA protocol exceeds the performances of other protocols from the perspectives of the accuracy of the data, the reliability of the routing path, the consumption of energy, and the lifetime of secure data aggregation.

1. **Introduction**

A wireless sensor network (WSN) is a highly distributed network composed of sensor nodes with special capabilities, and they are deployed in large-scale area to monitor the environment and collect related information [1–4]. Recently, the use of WSNs has become more popular and promising in various research areas, such as environmental monitoring [4–7], military target tracking [8, 9], natural disaster relief [10], and health monitoring [11]. WSNs have become one of the key modern information technologies, and the technology is changing people's lives and the way people interact with the physical world.

Generally, sensor nodes are deployed so densely that the sensing scales of neighboring nodes often have serious overlaps, resulting in redundant sensing of data and unnecessary expense in correlating the same data. The amount of data received by the base station is much greater than necessary. Data-aggregation technology [12, 13] is used to process the raw data, eliminate redundant or superfluous data, and save energy by ensuring that the network works efficiently. Obviously, the security of WSNs must be taken into consideration when they are deployed in insecure and hostile environments, so secure data-aggregation gradually is becoming a key technology. There are several approaches to keep the data-aggregation process secure [14], such as cryptography, key management, authentication mechanisms, privacy-preserving technologies, and reputation-based mechanisms. To the best of our knowledge, cryptographic-based technologies generally are utilized to keep the network free from the attacks during the data-aggregation process. However, the security of data-aggregation cannot be guaranteed by pure cryptography, because cryptographic-based technologies cannot provide adequate defense against node capture attack that results in the occurrence of compromised nodes. Compromised nodes allow easy access to the cryptographic keys that are used for cryptographic-based data-aggregation, and, when such access occurs, it cannot be detected.

To overcome the shortcoming of cryptographic-based secure data-aggregation, reputation and trust systems are
being developed to complement existing technologies for monitoring network activities and events. Reputation and trust systems are utilized to detect, collect, process, and disseminate feedback concerning the sensors’ recent behaviors and to assess their trustworthiness for specific applications. The goals of using such systems are to defend against node capture attack that results in the occurrence of compromised nodes, identified nodes that have been compromised, and exclude them from further participation in data-aggregation. The trustworthiness of sensors is evaluated based on their various activities, including data collection, data transmission, aggregator selection, and routing path selection. The reputation of each node refers to the expectation of neighboring nodes concerning a node’s behavior based on their observations of its past actions. Thus, trust and reputation in a WSN often are mentioned together. Therefore, a node’s reputation will affect its choices and activities. Trust of a node generally is defined as the expected value of that node’s reputation.

In this paper, we propose an improved reliable, trust-based, and energy-efficient data-aggregation protocol for WSNs. We call the protocol the iRTEDA protocol, and simulations have shown that the iRTEDA protocol exceeds the performances of other protocols from the perspectives of the accuracy of the data, the reliability of the routing path, the consumption of energy, and the lifetime of secure data-aggregation. It improves Suat Ozdemir’s RDAT protocol [15, 16] and provides information concerning residual energy and link availability to evaluate the trustworthiness and reliability of sensor nodes based on the observations of neighboring nodes. The iRTEDA protocol uses a reputation function that is based on a Beta distribution to assess the reputation and trustworthiness of nodes in performing their tasks. Information concerning the residual energy and link availability of the nodes was introduced to help the network reselect the aggregators and improve the robustness of the selected routing path, when the aggregators are judged as compromised nodes. In addition, a recovery mechanism is proposed in the iRTEDA protocol to keep nodes from becoming isolated, improve the structure of the clusters, and reduce the energy consumed for data transmission after the compromised nodes have been excluded.

The organization of the paper is listed in the following. Section 2 introduces previous works about trust-based systems in wireless sensor networks. Descriptions of system model, Beta reputation system, and problem statement are provided in Section 3. Section 4 proposes improved reliable, trust-based, and energy-efficient data-aggregation. Performance evaluation and analysis are described in Section 5. Section 6 is the conclusions.

2. Related Work

In this section, previous work is presented to introduce the development of trust-based system for WSNs. In accordance with the characteristics of WSNs, centralized trust-based systems are not feasible because there is a centralized trusted center that controls the systems in the network. As the domain grows, one centralized trusted center can reduce the scalability and expandability of the network. Thus, decentralized trust-based systems are being developed and used in WSNs. Recently, trust-based systems that are used in WSNs have been divided into five types according to their different applications, that is, generic, routing, access, location, and aggregation. In [17, 18], Boukerche and Ren proposed a trust computation and management system (TOMS) that develops a generic trust model to evaluate all the actions of the nodes, including making credential assignments, managing the trust values of the nodes, updating the keys, and judging the actions of the nodes to decide their access rights. Similar to Boukerche et al’s scheme, RFSN [19, 20] first combines first-hand and second-hand information to compute the reputation and trust values of the nodes and then develops a general, trust-based model. In [21], Shaikh et al. proposed a hybrid trust management architecture for clustered WSNs, which they called GTMS. Their scheme divided the evaluation of the reputation values into three levels, that is, sensor node, cluster head, and base station. The innovation of the GTMS scheme was that it eliminated the use of one single reputation value to evaluate the actions of the nodes by dividing the evaluations of the reputation and trust values into three levels according to the architecture of the network. Michiardi et al. [22] and Srinivasan et al. [23] developed special trust-based models, referred to as CORE and DRBTS, to prevent nodes from exhibiting selfish behavior and to exclude compromised nodes just for routing and location, respectively. Compared with the models above, RDAT protocol [15, 16] introduced multiple functions to compute the reputation and trust values based on three specific aspects, that is, sensing, aggregating, and routing. The protocol combines the evaluation of these three aspects to evaluate the trustworthiness of nodes. Our proposed scheme is based on the RDAT protocol, but it has significant and beneficial advantages over that protocol because it considers energy efficiency, link availability, reselection of aggregators, and recovery mechanisms.

3. Preliminary

3.1. System Model. In this paper, the hierarchical cluster architecture was used to construct WSNs composed of sensor nodes that were densely deployed in clusters. It was assumed that the operation of each cluster was relatively independent and that very few, if any, nonoverlapping areas would be sensed between the clusters. Hence, the reputation and trust of the sensor nodes are evaluated only by the nodes in their own cluster. A watchdog mechanism is used to monitor and detect the actions of target nodes, and those actions are characterized as cooperative or noncooperative; judgments are made concerning whether the action of the nodes are right or not. Thus, the reputation and trust system is responsible for maintaining the reputation and trust of a node, and this duty includes many tasks. The system updates reputation information based on new observations made by the watchdog mechanism and creates new evaluations of the trustworthiness of the nodes.

Each cluster has a cluster head called an aggregator, which is in charge of a certain number of sensor nodes
and has the capability of performing the data-aggregation operation. Aggregators are utilized to process received data from children nodes and transmit the aggregated results to base station. Sensor nodes, with the exception of the aggregator, sense the data, monitor the activities of other nodes, exchange observations with neighboring nodes, evaluate the trustworthiness of the nodes, and transmit data and observations to the aggregator. When the sensor nodes report their readings to the aggregators, the messages are encrypted and decrypted by pairwise keys that are generated and that are possessed only by the two communicating parties through their negotiation. In addition, the aggregators, namely, the cluster heads that are in the hierarchal cluster architecture, are not maintained for a long term and dynamically changing, because, when the system is running, adversaries can follow the aggregators more and more closely, so security problems associated with those aggregators will increase. In addition, the energy consumption of those aggregators increases rapidly and significantly when they remain unchanged for extended periods. Thus, to solve the security and energy problem, sensor nodes in the cluster must be reselected dynamically as aggregators at intervals.

3.2. Beta Reputation System. Reputation and trust systems are used extensively in various domains for WSNs, such as gathering, sharing, and modeling information, routing, decision making, and dissemination, which help the network identify malicious and compromised nodes and eliminate their adverse effects. Sensor nodes use the watchdog mechanism to monitor the behaviors of neighboring nodes and to decide whether those behaviors are acceptable or not. Then, the information obtained about the activities of the sensor nodes is used to evaluate the trustworthiness of the nodes and to decide whether possible compromised nodes exist.

In [19, 20], the researchers proposed that the use of a binary rating for the behaviors of sensor nodes was adequate for the data-aggregation operation, because their activities were evaluated as only good or bad. Therefore, a Bayesian formulation, called the Beta reputation system, was introduced to represent and update the trust of sensor nodes. This system can be expressed as

\[ P(\varphi | \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) \cdot \Gamma(\beta)} \varphi^{\alpha-1}(1-\varphi)^{\beta-1}, \]  

(1)

\[ 0 \leq \varphi \leq 1, \quad \alpha > 0, \quad \beta > 0. \]

The parameter \( \varphi \) is the probability that binary events will occur, and \( P(\varphi | \alpha, \beta) \) represents the distributions determined by the parameters \( \alpha, \beta \), and the gamma function, \( \Gamma \). The probability expectation of this distribution \( P(\varphi | \alpha, \beta) \) is given in [24] as

\[ E(\varphi) = \frac{\alpha}{\alpha + \beta}. \]  

(2)

The function is based on the theory of statistics, and it scales the values in the interval with any condition, even for any peaking time.

Now, we present a description of how the Beta reputation system works in WSNs. Consider that there are two nodes, \( i \) and \( j \), in the network. Each node detects and monitors the action of the other node, and they use their observations to update their reputation and trust. For simplicity, it is assumed that node \( j \) is the target node and that node \( i \) is the detecting node. Since the Beta reputation system is used as the binary rating function for the behaviors of the sensor nodes, detecting node \( i \)'s observation of the action of target node \( j \) is divided into two categories, that is, correct and false. Let \( m \) be the number of correct behaviors of target node \( j \), and let \( n \) be the number of false behaviors. Then, the parameters \( \alpha, \beta \) in the Beta function are set as follows:

\[ \alpha = m + 1, \quad \beta = n + 1, \quad m, n \geq 0. \]  

(3)

Therefore, the variable \( \varphi \) is redefined as correct observation the target node, while \( P(\varphi | \alpha, \beta) \) is the probability that \( \varphi \) has a special value. The probability expectation \( E(\varphi) \) may be expressed as the most likely value of the variable \( \varphi \). Then, we discuss the values of the probability expectation \( E(\varphi) \), including three possible conditions as follows:

\[ (1) \quad \alpha = \beta, \quad E(\varphi) = \frac{\alpha}{\alpha + \beta} = 0.5, \]

(4)

\[ (2) \quad \alpha < \beta, \quad E(\varphi) = \frac{\alpha}{\alpha + \beta} = \frac{1}{1 + \beta/\alpha} < 0.5, \]  

(5)

\[ (3) \quad \alpha > \beta, \quad E(\varphi) = \frac{\alpha}{\alpha + \beta} = \frac{1}{1 + \beta/\alpha} > 0.5. \]

(6)

(1) When \( \alpha = \beta \), \( E(\varphi) = 0.5 \). The number of correct behaviors of the target node is equal to the number of false behaviors. The result shows that the probability that target node is legal is the same as the probability that it is not; that is, it has been compromised.

(2) When \( \alpha < \beta \), \( E(\varphi) < 0.5 \). The number of correct behaviors of the target node is less than the number of false behaviors. This result indicates that the probability that target node has been compromised is greater than the probability that it is a legal node.

(3) When \( \alpha > \beta \), \( E(\varphi) > 0.5 \). The result indicates the opposite of the condition in (2), where the condition was \( \alpha < \beta \).

In addition to those described above, normal sensor nodes and aggregators will store their observations of neighboring nodes in a table and exchange the table with neighboring nodes. In this way, the nodes will combine first-hand and second-hand information to evaluate reputation and trust. Then, the network can use the trust to judge whether the aggregators and normal sensor nodes are compromised.

3.3. Problem Statement. The RDAT protocol first was proposed in [15, 16] to achieve the operation of reliable data-aggregation and transmission based on the reputation system. It combines the reputation functions of sensing, aggregating, and routing to achieve the security of data-aggregation
operation. However, security issues in RDAT are focused only on reputation and trust. During data transmission, the aggregators select the routing path and forward the aggregated results to base station along that path. However, security issues can occur when the same secure routing paths are used repeatedly. Some nodes in those paths will consume excessive energy, and others will consume little energy, resulting in the disruption of the balance of energy consumption and shortening of the lifetime of the network. In addition, when aggregators or normal sensors are judged as compromised nodes by the reputation and trust system, a recovery operation must be used for those nodes. Therefore, the focal points of our work are to incorporate in the reputation and trust system with nodes’ residual energy, link availability between nodes, and recovery mechanism to achieve a more secure, reliable, and energy-efficient data-aggregation operation.

4. Improved Reliable Trust-Based and Energy-Efficient Secure Data-Aggregation

Our proposed iRTEDA protocol is developing from RDAT and improving the problem that occurs in protocol RDAT. The basic idea of iRTEDA protocol is to combine reputation and trust system, nodes’ energy consumption, robustness of selecting routing path, and a recovery mechanism to decrease energy consumption and keep data-aggregation more reliable, when sensor nodes are compromised. Let us introduce iRTEDA protocol in detail as follows.

4.1. Reputation and Trust Computation. In the proposed iRTEDA protocol, the reputation and trust system defines the tasks of the nodes as sensing, aggregating and routing, and evaluating the trustworthiness of each task based on first-hand and second-hand information. It is assumed that there is a cluster that is composed of a group of sensor nodes, \( N_k \) \((k = 1, 2, \ldots, n)\). Node \( N_j \) is assigned to evaluate the reputation and trust for the tasks of its neighboring node \( N_i \) in the cluster. It monitors the actions of node \( N_j \), decides whether the actions are good or bad, and records the judgments in an observation table. The information recorded in the table by node \( N_j \) is the first-hand information for node \( N_j \). First-hand information, as the name suggests, is the information in the reputation table about neighboring node \( N_i \) that is observed and recorded by node \( N_j \). At the same time, the other nodes in the cluster also have recorded their judgments of node \( N_j \)'s tasks in their own observation tables.

Then, the information regarding node \( N_j \) in the observation tables is exchanged between nodes. Node \( N_j \) receives the observation tables from other nodes in the cluster and obtains neighboring nodes' observations of node \( N_i \). The information about node \( N_i \) in the other nodes' observation tables is second-hand information for node \( N_j \). The observation tables are exchanged in two ways, that is, on demand and broadcasting. The on demand procedure takes place when node \( N_i \) requests that neighboring nodes exchange observation tables with it and uses the observations to evaluate the reputation of \( N_i \). Broadcasting refers to the case in which the nodes broadcast their observation tables for a certain time period. For the sake of simplicity, in this paper, we used broadcasting to exchange the reputation tables.

Calculating trust for the actions of one node based on first-hand and second-hand information is introduced in the following. The task of sensing is taken as an example for the explanation of the reputation and trust evaluation. When the node \( N_j \) is detecting and monitoring the sensing task of node \( N_i \), the numbers of behaviors and misbehaviors of node \( N_j \), as judged by node \( N_j \), are recorded as \( \alpha_{ij}^{\text{new}} \) and \( \beta_{ij}^{\text{new}} \), respectively. Reputation value and trust for the sensing task of node \( N_j \) are represented by \( R_{ij}^{\text{sensing}} \) and \( T_{ij}^{\text{sensing}} \), respectively. The formula of reputation and trust calculation is

\[
R_{ij}^{\text{sensing}} = \text{Beta} \left( \alpha_{ij}^{\text{new}} + 1, \beta_{ij}^{\text{new}} + 1 \right)
\]

\[
= \frac{\Gamma (\alpha_{ij}^{\text{new}} + 1) + \beta_{ij}^{\text{new}}}{\Gamma (\alpha_{ij}^{\text{new}} + 1) + \beta_{ij}^{\text{new}} + 1} \cdot \frac{\Gamma (\beta_{ij}^{\text{new}} + 1)(1 - \varphi)}{\varphi (\alpha_{ij}^{\text{new}} + 1) - 1}.
\]

(5)

\[
T_{ij}^{\text{sensing}} = E \left( R_{ij}^{\text{sensing}} \right) = \frac{\alpha_{ij}^{\text{new}} + 1}{\alpha_{ij}^{\text{new}} + \beta_{ij}^{\text{new}} + 2}.
\]

(6)

The parameters \( \alpha_{ij}^{\text{new}} \) and \( \beta_{ij}^{\text{new}} \) are the new numbers of correct and false actions of node \( N_j \) calculated by first-hand and second-hand information. The process of integrating first-hand and second-hand information into an overall reputation was proposed in [16, 19, 20], and it is shown below:

\[
\alpha_{ij}^{\text{new}} = p \cdot \alpha_{ij}^{\text{now}} + m_{ij} + \sum_{k \in N} R(m_{k,j}),
\]

\[
\beta_{ij}^{\text{new}} = p \cdot \beta_{ij}^{\text{now}} + n_{ij} + \sum_{k \in N} R(n_{k,j}),
\]

(7)

where parameters \( \alpha_{ij}^{\text{now}} \) and \( \beta_{ij}^{\text{now}} \) are the last observations about correct and bad actions of node \( N_j \) in the observation table, respectively, and \( m_{ij} \) and \( n_{ij} \) represent the number of recent observations of correct and bad sensing actions, respectively. Old feedback cannot always work effectively for the new reputation and trust rating during the operation, so the old observations are less important than most recent observations, and they will be eliminated gradually. Therefore, the elimination parameter \( p < 1 \) is introduced to achieve the characteristic of last observations described above. In addition, second-hand information is exchanged between node \( N_i \) and \( N_k \) \((k = 1, 2, \ldots, n)\), and the observed numbers of correct and bad behaviors are expressed as \( R(m_{k,j}) \) and \( R(n_{k,j}) \) \((k = 1, 2, \ldots, n)\), respectively. Second-hand information for correct and bad actions is defined in [20] and is shown below:

\[
R(m_{k,j}) = \frac{2 \cdot \alpha_{ij}^{\text{new}} + \beta_{ij}^{\text{new}} + 1}{2 \cdot \alpha_{ij}^{\text{now}} + \beta_{ij}^{\text{now}} + 1},
\]

\[
R(n_{k,j}) = \frac{2 \cdot \beta_{ij}^{\text{new}} + \alpha_{ij}^{\text{new}} + 1}{2 \cdot \beta_{ij}^{\text{now}} + \alpha_{ij}^{\text{now}} + 1}.
\]

(8)
Then, we can compute node $N_j$’s trust $T_{i,j}^{\text{sensing}}$ about the sensing task using formula (6). According to the value of node $N_j$’s trust, node $N_i$ can use formula (4) to make the judgment about whether node $N_j$ is compromised. Node $N_i$ will transmit the judgment to the aggregator in the cluster. The aggregator receives the judgment about Node $N_j$ from other nodes in the cluster and decides whether node $N_j$ is compromised. If node $N_j$ is a compromised node, the aggregator will exclude node $N_j$ from the network and use the measures to eliminate compromised node $N_j$’s negative effects.

4.2. Residual Energy and Link Availability. The rating system above is based on reputation and trust, and it only pays attention to the reputation of sensing, routing, and aggregating actions; it cannot guarantee that the energy consumed by the sensor nodes is reasonable. Nodes with high reputations, which are selected for routing paths, will be utilized repeatedly, and they will take much more energy than those with low reputations. Obviously, selecting nodes for routing paths based only on their reputation and trust system ignores the nodes’ energy usage. That will result in the repeated selection of nodes with high reputation, and these nodes will be overused for forwarding the data, disrupting the equilibrium of nodes’ energy consumption. The nodes in the paths use up their energy rapidly, and others consume less energy, and this leads to significant differences between the energy consumptions of the nodes and decreases the lifetime of the network. Therefore, the residual energy and link availability between nodes must be taken into consideration and combined with the reputation and trust system to keep the network secure, reliable, and energy-efficient.

Sensor nodes in the routing path, in addition to their sensing task, must relay data towards the aggregators and base station. Sensor nodes and aggregators record their residual energy and exchange this information with neighboring nodes. Then, the nodes can use the energy information to determine the link availability between them. Thus, the aggregators also can obtain the status of the energy levels of the nodes in their cluster and identify the best nodes for forwarding data to the base station. Energy tables and reputation tables are exchanged simultaneously, and, when they are received, there are two advantages in the data-aggregation operation; that is, (1) in each cluster, nodes can select the best aggregator of the cluster in a certain time period according to reputation and energy information. The selection requires the consensus of all the nodes’ points and is determined based on the equilibrium of reputation and energy, and (2) after the aggregation is completed in each cluster, then results of the aggregation are transmitted to the base station along the routing path. Combining reputation and energy information could confirm link availability between nodes and identify a better path from each aggregator to the base station. It is also useful to select the best path from the sensor nodes to their clusters’ aggregators.

The parameter $N_{ET}$ is defined below to represent a node’s combined information of reputation and energy. It takes both reputation and energy into consideration and is used to judge whether a node’s trust and energy are sufficient for it to be an eligible aggregator or a routing node. Calculating the parameter $N_{ET}$ helps the system identify the best aggregator and routing nodes in each cluster:

$$N_{ET} = \frac{E \times T}{\text{Init} - E \times \text{Init} - T}, \quad E > \theta_{Eg}^A, \quad T > \theta_{T}^A,$$

where $N_{ET}$ is the parameter that combines reputation and energy for each node.

Then, we define the link availability $L_{AB}$ between node $A$ and $B$ in the following:

$$L_{AB} = \frac{\text{Init} - T_{AB} \cdot \text{Init} - E_{B}}{T_{AB} \cdot E_{B}}, \quad E_B > \theta_{Eg}^{\text{relay-node}}, \quad T_{AB} > \theta_{T}^{\text{link}},$$

where $T_{AB}$ represents the reputation of node $B$ evaluated by node $A$, $E_B$ is the residual energy of node $B$, $\theta_{Eg}^{\text{relay-node}}$ is the minimum value of the residual energy of node $B$ to transmit the data, and $\theta_{T}^{\text{link}}$ is the minimum acceptable value for trust of link, which is node $B$’s reputation as evaluated by node $A$.

Assume that there are $p$ two-hop nodes with link availability in the routing path between $i$ and $j$, each with the middle nodes $s_l (1 < l < p)$, and denote $L(i, j)$ as the link availability of nodes between $i$ and $j$. The whole link availability between $i$ and $j$ is denoted as $\text{Link}(i, j)$:

$$\text{Link}(i, j) = L(i, j) + \sum_{l=1}^{p} \min(L(i, s_l), L(s_l, j)).$$

In addition, each node $i$ assigns a weight to all its linked neighbors that are closer to the sink than it is. We denote $U(i)$ as the set of node $i$’s neighbors’ link availability. And recall $\text{Link}(i, j)$ is the link availability between node $i$ and $j$. We assign link availability to each node $j$ in set $U(i)$ as

$$w_j = \frac{\text{Link}(i, j)^{\alpha}}{\sum_{m \in U(i)} \text{Link}(i, m)^{\alpha}},$$

where $w_j$ is the link availability that $i$ chooses $j$ as the forwarder. When $\alpha = 0$, all nodes in $U(i)$ are given equal priority regardless of link resilience. When $\alpha$ is positive, the more resilient links are given higher priority. When $\alpha$ approaches infinity, only the more resilient links are chosen for routing. An intermediate value can be used to achieve a good balance between security and lifetime. Therefore, to choose a neighbor on the secure and reliable path to the base station, we use $U(i)$ as the set of link availability of node $i$ to decide whether the nodes are linked reliably to be on the routing path. If there is a need for balance between security and lifetime, a weight $w_j$ can be set to each of its link neighbors $j$ in the set $U(i)$. In order to simplify the analysis of our protocol in the following, we will set the parameter $\alpha = 0$ and the weight $w_j = 1$.

The network uses residual energy and link availability to reselect the aggregators and routing paths every $T_s$ time period. It is possible that some links between nodes will fail during the time period. So this operation is done each $T_s$ time period, and the new information of new aggregators and new upstream nodes in the cluster is shared and recorded.
4.3. Recovery Mechanism. After the computation of reputation and trust, the aggregators could determine and judge whether neighboring nodes are compromised or not. Once the nodes are judged as compromised nodes, those nodes will be excluded from the network. Their father nodes no longer receive data from the compromised nodes, and their children nodes do not forward data to them. After compromised nodes are marked and excluded, the structure of the network will be adjusted to guarantee that compromised nodes' children nodes find the right father nodes to keep these children nodes from becoming isolated nodes. Thus, a recovery mechanism is required to keep compromised nodes' children nodes from becoming isolated. The structure of a cluster in a WSN is shown in Figure 1. The entire network consists of the base station, aggregators, and the sensor nodes. Each aggregator, namely, the cluster head, manages all the sensor nodes in the cluster. In the following, the recovery mechanism is shown for different situations.

(1) Leaf Node Is Compromised. When the aggregator makes an evaluation that a leaf node is a compromised node, the aggregator will send messages to the sensor nodes in the cluster instructing them to ignore the compromised node’s messages and to exclude it from the cluster. After that, the aggregator also will send warning messages to the aggregators in the neighboring clusters. In Figure 2, aggregator \( AG_1 \) makes a judgment that leaf node \( SN_7 \) has been compromised and excluded from the cluster. Then, aggregator \( AG_1 \) sends warning messages to the other aggregators \( AG_2 \) and \( AG_3 \). After those aggregators receive the warning messages, they will take precautions against compromised node \( SN_7 \) and ignore its messages.

(2) Intermediate Node Is Compromised. When an intermediate node is judged to be a compromised node, the aggregator excludes the compromised node from this cluster and sends warning messages to this node's children nodes. Its children nodes will become isolated and tend to find candidate father nodes. If a child node cannot find its candidate father node, it will check its ID list and look for uncle nodes that were stored in the invitation message received from the cluster heads when the cluster structure was built. The node will send a request message to its uncle nodes asking to join their clusters and wait for their responses. When children nodes are authenticated legally by uncle nodes, a response will be transmitted to the children nodes admitting them to the cluster. This operation makes children nodes reselect a father node, reduces the hops to the base station, and reduces the energy required for communication during the transmission of data. The operation is shown in Figure 3. Aggregator \( AG_2 \) makes a judgment that intermediate node \( SN_4 \) has been compromised. Then node \( SN_4 \)'s children nodes \( SN_9 \) and \( SN_{10} \) send request messages to their uncle nodes \( SN_3 \) and \( SN_5 \). When the legality of \( SN_9 \) and \( SN_{10} \) has been guaranteed by \( SN_3 \) and \( SN_5 \), they will join the cluster managed by \( SN_3 \) and \( SN_5 \).

(3) Aggregator Is Compromised. When the network determines that the aggregator is compromised, the aggregator will be reselected by nodes in the cluster. Reselecting the aggregator must involve evaluating the nodes’ reputations and residual energies simultaneously and balancing the two aspects. Figure 4 shows that aggregator \( AG_1 \) is judged as a compromised node and excluded from the cluster. Neighboring clusters will be informed of the decision about compromised aggregator \( AG_1 \). Then, all the nodes in this cluster will exchange reputation and residual energy tables and combine reputation and residual energy to decide which node is most appropriate to be the aggregator in next time period. In Figure 4, sensor node \( SN_5 \) is selected as the new aggregator, and it collects the messages from other...
sensornodesintheclusterandexecutesthedata-aggregation
operation.

(4) Node in the Routing Path Is Compromised. When node
CN in the routing path is compromised, the subsequent
operation is shown in Figure 5. The solid line is the original
routing path, and the broken lines are the lines that may
possibly be reselected to join the routing paths. In order to
prevent forwarding and misdirecting attacks launched by a
compromised node, the recovery mechanism makes a reliable
multipath for data transmission after the compromised nodes
are identified. It ensures that the nodes reselect reliable nodes,
from the perspectives of trust and energy path, to transmit
and route the data to the base station. The reselection of
the routing path is based on trust, residual energy, and link
availability, which keeps the quantity of reselected paths and
excludes compromised nodes from the routing paths. To
perform the recovery mechanism, each data aggregator must
determine the possible paths to the base station and decide
which path will be reselected to transmit the aggregated data.

5. Performance Evaluation

To evaluate the performance of the proposed iRTEDA pro-
tocol, we compared it with the RDAT protocol for different
aspects, including average reputation values, data accuracy,
routing path reliability, energy consumption, and lifetime.
Both protocols were developed by using the Tiny OS 2.0
simulator (TOSSIM) and its variant, PowerTOSSIM. Energy
is a crucial constraint in wireless sensor networks. It is an
important issue in performance evaluation. So we use TinyOS
simulator PowerTOSSIM, a power modeling extension to
TOSSIM. PowerTOSSIM accurately models power consumed
by TinyOS applications. One hundred sensor nodes were
deployed in the network that had an area of 300 m × 300 m.
The sensor nodes were distributed in different areas and
organized based on the structure of the cluster. The base
station was located in the central area, and each cluster had
an aggregating node for the cluster header. A fixed number of
nodes were assumed to be compromised. They transmitted
false data to the aggregators, which aggregated the false data
in to the transmitted data and selectively forwarded it to base
station. In addition, link failure and packet loss were set as
fixed values to better represent practical situations in a WSN.

5.1. Comparison of Reputation Value. In the section, we
used average reputation values to assess reputation and trust
system based on the statistics associated with the running
time period of the network. There were 30% of compromised
nodes in the network to provide sensing misbehaviors. So nodes should monitor and detect the misbehaviors of their neighboring nodes and compute those nodes’ average reputation values. Figure 6 shows the average reputation values $R_{sensing}^{i,j}$ of the compromised and the legitimate nodes’ sensing actions. We used those values to evaluate the nodes’ trustworthiness. From Figure 6, it was concluded that the variation tendency of average reputation value for legitimate and compromised nodes in both protocols was almost the same because average reputation values $R_{sensing}^{i,j}$ were assessed by combining first-hand and second-hand information in both protocols. The compromised nodes cannot hide their sensing misbehaviors to get higher average reputation values. So, the compromised nodes’ average reputation value was reduced in stages until the ultimate value was reached. However, as Figure 6 shows, the average reputation values of the legitimate nodes in iRTEDA protocol always were lower than those of the RDAT protocol. This occurred because iRTEDA protocol evaluated the nodes’ average reputation values based on the nodes’ behaviors and misbehaviors as well as taking residual energy and link availability into consideration. The evaluation standard will result in decreasing the security and average reputation values of nodes in the routing path, but it leads to better energy efficiency, stability, and reliability.

5.2. Comparison of Data-Aggregation. The accuracy of data-aggregation always has been regarded as a crucial criterion for aggregation performance in the network. It is denoted in this section the ratio of the sum of the data from legal nodes collected by the base station to the sum of all of the data collected by the base station. In the cluster, the data sensed by normal nodes are transmitted to the aggregators, and they are aggregated. When the aggregators are compromised, the results they produce become unbelievable. Figure 7 shows the increasing trend of aggregating accuracy for the RDAT protocol and our proposed protocol. Initially, the aggregating accuracies of both protocols increase at slow rates because the systems were just beginning to work, and the compromised nodes’ misbehaviors were not detected yet, meaning they were not excluded from the network. When the reputation and trust system is running, the aggregating accuracy increases sharply when the running time is in the range of 500 to 1500 s. The aggregating accuracy of the iRTEDA protocol increased to almost 83%, whereas the RDAT protocol increased to about 80%. This is because the reputation system began to work and excluded the compromised nodes from the network. The aggregating results received by the base station belonged to the legal nodes to a greater extent as time passed. When the running time of about 1500 s was reached, the rate of growth of the aggregating accuracy slowed significantly. However, the final aggregating accuracy for the iRTEDA protocol was greater than that of the RDAT protocol. This occurred because the RDAT protocol does not pay enough attention to the energy and link availability issues, and this results in a greater death rate of nodes, meaning that the base station received less data from legal nodes. In addition, the recovery mechanism ensures that isolated legal nodes can rejoin the network and find a high-reputation parent node. This mechanism will increase the number of legal nodes that finally are received by the base station in the iRTEDA protocol.

5.3. Comparison of Routing Path Reliability. The routing-path reliability metric is defined as the ratio of the sums
of the amounts of sensing data and the aggregating results received by the aggregators and the base station to the total amount of transmitted data. The aggregators eliminate a lot of redundant data. Thus, the reliability of the routing-path should be compared in two ways, that is, normal nodes to aggregators and aggregators to the base station. The issues that may influence the performance of routing-path reliability are including link availability and residual energy. As seen in Figure 8, with the network running, the percentage of failed links increased. The number of failed links in the RDAT protocol increased much more quickly than that in the iRTEDA protocol. The reason for this was that the RDAT protocol does not consider residual energy, and it does not have a recovery mechanism to keep the network running efficiently. The RDAT protocol only considers reputation, which leads to excessive use of nodes that have been assessed as having higher reputation. Such nodes consume more energy, and their death rate helps to balance the energy consumption of the nodes. Nodes with higher reputation will consume energy more quickly than others with low reputation, so they die much faster, which leads to higher failed links during data transmission. Figure 8 shows that the failed links in the RDAT protocol were similar to those in the iRTEDA protocol from the beginning to about 600 s. Because there is enough energy for nodes and aggregators in the beginning, few nodes are dead for using up the energy. During the time period, the fail links are occurring for the reason that some nodes have been compromised and excluded from the network. After the network has been running for 600 s, the number of failed links in the RDAT protocol is increasing much more rapidly that were in the iRTEDA protocol. Thus, in the RDAT protocol, the transmission of data among nodes, aggregators, and the base station became more and more unreliable with time. At the same time, the reliabilities of both protocols were significantly different when the network was running. Figure 9 shows that, when the failed links reached 30%, the reliability of RDAT and iRTEDA decreased to about 79.2% and 89.5%, respectively. The larger number of failed links is responsible for the lower reliability. With high unreliability of data transmission, there will be large amount of data loss, and data accuracy will decrease quickly. Thus, the iRTEDA protocol is more reliable for maintaining data transmission and improving the performance of data-aggregation, when the reputation system improves the security of the network.

5.4. Comparison of Energy Consumption. The concept of lifetime describes the death rate for the nodes in the network, which is defined as the number of dead nodes overtime. Energy consumption shows us the percentage of energy consumption of all the nodes in the network. Combining lifetime and energy consumption, we can obtain the detailed performance for the total energy consumption and energy balancing of nodes. Figure 10 shows that the death rates of nodes in the two protocols were significantly different. The death rate of nodes in RDAT was much faster than it was in our protocol. There is a large number of dead nodes in the beginning. The reason is that, in RDAT, there are excessive uses for those nodes with higher reputation in routing and transmission, which results in quick death for those nodes.

With the network running for more than 2000 seconds, the nodes with lower reputation, isolated nodes, and the death rate are decreased to very low rates. The selection of the nodes in routing and transmission in our protocol was based on reputation, but it also emphasized energy consumption and link availability. Thus, unlike the RDAT protocol, it will not lead to excessive use of the same nodes, and it provides better energy balancing. All of the energy that is consumed will be distributed over large number of nodes in iRTEDA protocol, instead of that all of the energy consumption will focused on few nodes with high reputations and those nodes consume...
energy more rapidly. Figure 10 shows that the death rate of nodes in our protocol was much lower than that in the RDAT protocol in the beginning, and the rate increased rapidly at a running time of 2500 s. Because more energy is consumed for each node after that time period, the death of nodes will increase as long as the network keeps running. When the network had operated for 4000 s, only six nodes were left in the RDAT protocol, whereas 20 nodes were left in our protocol.

Figure 11 compares the entire energy consumptions of the two protocols. Before about 2500 s, the rate of increase in energy consumption was much lower in iRTEDA than in RDAT, with iRTEDA reaching about 43.6% and RDAT reaching about 90.1%. The difference in the energy consumption of the two protocols was caused by the proposed recovery mechanism, because the nodes with low reputation are judged as compromised nodes and excluded from the network. Those compromised nodes’ children nodes will become isolated. Those isolated nodes transmit data directly to the base station and consume much more energy than before. Thus, the recovery mechanism will help the dispersing or isolated nodes in the network finish the reselection of father nodes and re-access to the clusters. This will lead to decreases in the average hops from those nodes to the base station which will save communication overhead and reduce the total energy consumption. At a running time of 4000 seconds, the percentage of energy consumption was about 93.4% for the RDAT protocol and about 83.8% for the iRTEDA protocol. Figure 11 shows that the total energy consumption was much lower for the iRTEDA protocol than for the RDAT protocol.

6. Conclusion

An improved data aggregation method for WSNs is presented in this paper. The method is reliable, trust-based, energy-efficient, and secure. The iRTEDA protocol combines residual energy and links availability to improve trust-based data-aggregation. Introducing residual energy and link availability facilitates the reputation system’s ability to keep aggregators and nodes in the routing path from being used excessively and guarantees that the routing path selected by the reputation system will be much more reliable. In addition, the recovery mechanism prevents compromised nodes’ children nodes from being isolated and helps those nodes to reselect new parent nodes. Simulation results showed that the proposed protocol outperformed the RDAT protocol with respect to its improved performance of data accuracy, routing path reliability, and the lifetime of data-aggregation, while reducing energy consumption. Thus, the proposed iRTEDA protocol achieved its goal of keeping secure data-aggregation in WSNs more reliable and energy-efficient.

Acknowledgments

This research is supported by National Natural Science Foundation of China Under Grant 61071076, Beijing Natural Science Foundation Under Grant 4132057, National High-tech Research And Development Plans (863 Program) Under Grant 2011AA010104-2, and The Academic Discipline and Postgraduate Education Project of Beijing Municipal Commission of Education.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–105, 2002.
[2] K. Römer, “Programming paradigms and middleware for sensor networks,” in Proceedings of the GI/ITG Workshop on Sensor Networks, pp. 49–54, Karlsruhe, Germany, 2004.
[3] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[4] D. Culler, D. Estrin, and M. Srivastava, “Overview of sensor networks,” Computer, vol. 37, no. 8, pp. 41–49, 2004.

[5] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, “Wireless sensor networks for habitat monitoring,” in Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA ’02), pp. 88–97, Atlanta, Ga, USA, September 2002.

[6] N. Xu, S. Rangwala, K. K. Chintalapudi et al., “A wireless sensor network for structural monitoring,” in Proceedings of the Second International Conference on Embedded Networked Sensor Systems (SenSys ’04), pp. 13–24, ACM Press, New York, NY, USA, November 2004.

[7] J. Polastre, R. Szewczyk, A. Mainwaring, D. Culler, and J. Anderson, “Analysis of wireless sensor networks for habitat monitoring,” Wireless Sensor Networks, vol. 4, pp. 399–423, 2004.

[8] T. He, P. Vicaire, T. Yant et al., “Achieving real-time target tracking using wireless sensor networks,” in 12th IEEE Real-Time and Embedded Technology and Applications Symposium (RTS ’06), pp. 37–48, San Jose, Calif, USA, April 2006.

[9] G. Simon, G. Balogh, G. Pap et al., “Sensor network-based countersniper system,” in Proceedings of the Second International Conference on Embedded Networked Sensor Systems (SenSys ’04), pp. 1–12, Baltimore, Md, USA, November 2004.

[10] E. Cayirci and T. Coplu, “SENDROM: sensor networks for disaster relief operations management,” Wireless Networks, vol. 13, no. 3, pp. 409–423, 2007.

[11] A. Milenković, C. Otto, and E. Jovanov, “Wireless sensor networks for personal health monitoring: issues and an implementation,” Computer Communications, vol. 29, no. 13–14, pp. 2521–2533, 2006.

[12] K. Akkaya, M. Demirbas, and R. S. Aygun, “The impact of data aggregation on the performance of wireless sensor networks,” Wireless Communications and Mobile Computing, vol. 8, no. 2, pp. 171–193, 2008.

[13] R. Rajagopalan and P. K. Varshney, “Data aggregation techniques in sensor networks: a survey,” IEEE Communications Surveys and Tutorials, vol. 8, no. 4, pp. 48–63, 2006.

[14] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: a comprehensive overview,” Computer Networks, vol. 53, no. 12, pp. 2022–2037, 2009.

[15] S. Ozdemir, Functional reputation-based data aggregation for Wireless sensor networks, in 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communication (WiMob ’08), pp. 592–597, October 2008.

[16] S. Ozdemir, “Functional reputation based reliable data aggregation and transmission for wireless sensor networks,” Computer Communications, vol. 31, no. 17, pp. 3941–3953, 2008.

[17] A. Boukerche and Y. Ren, “A trust-based security system for ubiquitous and pervasive computing environments,” Computer Communications, vol. 31, no. 18, pp. 4343–4351, 2008.

[18] Y. Ren and A. Boukerche, “Modeling and managing the trust for wireless and mobile ad hoc networks,” in IEEE International Conference on Communications (ICC ’08), pp. 2129–2133, Beijing, China, May 2008.

[19] S. Ganeriwal and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” in Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN ’04), pp. 66–77, October 2004.