International Journal of Control and Automation
Vol.8, No.3 (2015), pp.305-318
http://dx.doi.org/10.14257/ijca.2015.8.3.31

An Energy-Efficient Reliable Trust-Based Data Aggregation Protocol for Wireless Sensor Networks

Teng Ma, Yun Liu* and Zhen-jiang Zhang

School of Electronic and Information Engineering, Key Laboratory of Communication and Information Systems, Beijing Municipal Commission of Education, Beijing Jiaotong University, Beijing, 100044, China
{08111003, liuyun, zhjzhang1}@bjtu.edu.cn*

Abstract

Security data aggregation plays an important role in reducing the amount of data transmission and prolonging the life of wireless sensor networks (WSN). When the security of the aggregation nodes is threatened, the networks can generate many aggregated data errors, leading to trouble in a security measure. In this paper, we propose an energy-efficient reliable trust-based data aggregation protocol for WSN called the ERTDA protocol. Based on the observations of the nodal behavior, the ERTDA protocol calculates, monitors and evaluates the trust values of the nodes; it also detects and excludes the compromised nodes in a timely manner. The simulation results illustrate that the ERTDA protocol can effectively improve the accuracy of the aggregation, reduce the nodal mortality rate, reduce the nodal energy consumption, improve the reliability of the data transmission and extend the life of the networks.

Keywords: *data aggregation, reputation, trust management mechanism, WSN*

1. Introduction

Wireless sensor networks (WSN) have been widely used in environmental monitoring, medical care, intelligent transportation, military reconnaissance, and logistics management [1-2]. WSN integrates information and the physical world closely to modify the interactions between humans and nature. Consequently, WSN have had a great influence on our lives.

The security data aggregation of WSN is the comprehensive application of two key technologies: data aggregation and security. This ensures the efficiency and security of the networks [3-4]. Traditionally, encryption is used to confidentially solve data aggregation security problems in WSN. Encryption can also be used for node authentication and access control in the process of data aggregation in WSN.

The cryptogram mechanism guarantees the confidentiality and integrity of data during a transmission to ensure that the cryptograph cannot be cracked by hostile nodes. However, the cryptogram mechanism is unable to resist internal attacks. With the continued operation of data aggregation, the importance of aggregation nodes gradually emerged. When the security of the aggregation nodes was found to be threatened, the networks would generate many aggregated data errors, yielding hidden troubles with security. As such, the security requirements of the data aggregation in WSN cannot be fully guaranteed when the reliance of the secure data aggregation protocol is solely based on encryption technology [5-7]. Consequently, ensuring the safety of the aggregation nodes, finding and eliminating the aggregation nodes that have been captured and preventing the compromised aggregation

ISSN: 2005-4297 IJCA

nodes from tampering with the aggregate data, can be solved by using the trust management mechanism.

A trust management mechanism can timely and effectively identify the compromised nodes and provide a decision-making framework for the problems of mutual trust between the nodes to effectively solve internal attacks. In conclusion, a trust management mechanism is an effective complement to the secure measures based on the cryptogram mechanism. In [8, 9], the authors proposed a secure data aggregation protocol (RDAT) based on the trust management model; the RDAT can effectively detect node invasion. Hence, these authors found that the compromised nodes could be captured and a secure data aggregation could be realized. In [10], the authors proposed the iRTEDA protocol. This iRTEDA protocol takes the energy of the nodes and the availability of the routing link into consideration. After precluding the compromised nodes, isolated nodes emerge. This results in a more secure and reliable aggregated data transmission. That being said, the threshold value in the iRTEDA protocol excessively relies on energy parameters, so there are some drawbacks. Motivated by secure data aggregation problems, in this paper, we propose an energy-efficient reliable trust-based data aggregation protocol for WSN called the ERTDA protocol. The simulations that we conducted to test our protocol illustrate that the ERTDA protocol can detect the compromised nodes in a more effective and timely manner. The ERTDA can also implement the data aggregation in a safer and more energy efficient way.

The rest of this paper is organized as follows. Section 2 introduces the previous work about the trust management mechanism and the Beta reputation system. Section 3 presents the ERTDA protocol. The performance evaluation is presented in Section 4, while the conclusions are made in Section 5.

2. Preliminary

2.1. Trust Management Mechanism

Reputation and trust is the foundation of the trust management mechanism. Reputation widely refers to the typical views and perspectives of a person, as well as whether they present themselves as having good or bad behavior [11]. On the computer, and more specifically, the wireless network system, reputation is often described as an expectation of other entities in terms of the future behavior of a certain entity within a given time period [12]. As such, the expectation depends on the observed information of other entities on the certain entity's behavior, as well as records of the certain entity's historic actions. Trust is defined in a given time period. It involves the environmental space of Entity A, through observation of Entity B, for a period of time. Combined with historical experience, a person can make a reliable and honest subjective judgment on the behavioral probability of performing some acts [13].

Trust and reputation are two different concepts, but they have a very close relationship [14]. The trust management mechanism is based on the subjective reputation of comprehensive information as an input. It then quantifies the results of the trust value as an output; this reflects the subjective judgment of an entity to another entity trust degree. Trust reflects the participation of the node on another node's honest subjective measurement, expressed as a mathematical expectation of reputation. Reputation, on the other hand, is a measure of the overall integrity of all of the nodes on the node, which is a random variable. In terms of the trust and reputation relationship, the trust of a node is determined by the reputation of that node.

Trust management mechanisms in WSN are primarily used to complete the following tasks:

(1). Monitoring and collecting a node's historical information, as well as its direct and indirect information.
(2). In accordance with the relevant model, to calculate the reputation value and the trust value of the nodes.
(3). The calculation results of the nodes' trust value compared with the preset trust threshold values, we take the corresponding measures for the nodes.

2.2. Beta Reputation System

In the trust management model, nodes observe the behavior of neighbors, according to the neighbor node behavior. This is conducted to estimate the reputation *p* and determine whether the current behavior of these nodes is correct.
The ERTDA model is the same as the iRTEDA model [10] in that it uses the Beta distribution [15] on the behavior of the sensor nodes to obtain the binary rating. There are two types of node behavior judgments: good and bad. This system can be expressed as:

$$P(\varphi \mid \alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\cdot\Gamma(\beta)} \varphi^{\alpha-1}(1-\varphi)^{\beta-1} \quad \text{where} \quad 0 \le \varphi \le 1,\ \alpha > 0,\ \beta > 0 \tag{1}$$

The parameter φ represents an event or an act on the Beta distribution; $P(\varphi \mid \alpha, \beta)$ represents the probability of the occurrence of the event or behavior, determined by the parameters α , β , and the gamma function Γ [16]. According to the theory of mathematical statistics, the expected value of the Beta distribution in the interval $[0,1]$ can be expressed as in Equation (2):

$$E(\varphi) = \frac{\alpha}{\alpha+\beta} \tag{2}$$

According to the characteristics in Formula 2, the application of the Beta model to the trust management model on the behavior of the sensor nodes binary rating, the reputation and trust values, is assessed. We then set the two nodes, *i* and *j*, to mutual monitoring and observe their behavior. We integrate the current status and history to update the reputation list of the destination nodes, where the node *j* is the destination node and the node *i* represents node *j's* behavioral monitoring and observation. The observation is judged using the Beta distribution and is divided into two actions: good and bad. Set *m* is the amount of observed good behavior obtained from the monitoring node *i* to the destination node *j*. *n* is the amount of observed bad behavior obtained from the monitoring node *i* to the destination node *j*. Parameters α and β are expressed as follows:

$$\alpha = m+1, \quad \beta = n+1, \quad m,n \ge 0 \tag{3}$$

According to the definition of the parameters, α and β , the parameter φ is redefined as the reputation value of the destination node *j*, $P(\varphi \mid \alpha, \beta)$ represents a certain probability of the destination node *j* for a certain reputation value, and $E(\varphi)$ represents the expectations of the reputation value φ by the destination node *j*, that represents the degree of trust on the observation node to the destination node.

We can now discuss the values of the probability expectation $E(\varphi)$, including the three possible conditions, as follows:

$$\alpha=\beta,\ E(\varphi)=\frac{\alpha}{\alpha+\beta}=0.5 \tag{4}$$

$$\alpha<\beta,\ E(\varphi)=\frac{\alpha}{\alpha+\beta}=\frac{1}{1+\beta/\alpha}<0.5 \tag{5}$$

$$\alpha>\beta,\ E(\varphi)=\frac{\alpha}{\alpha+\beta}=\frac{1}{1+\beta/\alpha}>0.5 \tag{6}$$

(1). When $m=n$, $\alpha=\beta$, and $E(\varphi)=0.5$, the amount of good behavior on the destination node is equal to the amount of bad behavior, where the trust value is 0.5. This result illustrates that the probability that the destination node is legal is the same as the probability that it is not.

(2). When $m<n$, $\alpha<\beta$, and $E(\varphi)<0.5$, the amount of good behavior of the destination node is less than the amount of bad behavior. The result shows that the probability that the destination node has been compromised is greater than the probability that it is a legal node.

(3). When $m>n$, $\alpha>\beta$, and $E(\varphi)>0.5$, the amount of good behavior of the destination node is more than the amount of bad behavior. The result illustrates that the probability that the destination node has been compromised is less than the probability that it is a legal node.

In addition to the content described previously, in the WSN, the nodes will store their observed information from the neighbor nodes in a table and exchange the information. In this way, the nodes will combine their own information with the observations of the neighboring nodes to evaluate the reputation and the trust values. Then the networks use the trust and the reputation values to determine which nodes are compromised.

2.3. Problem Statement

The RDAT protocol was based on the reputation system. It is used to realize the reliable data aggregation [8, 9] under the trust management mechanism that used the reputation and trust system, achieve the security aggregation node selection and determine the reliable data aggregation routing. However, in the RDAT protocol, the only focus is on reputation and trust. The RDAT protocol ignores the impact of the node energy for aggregation and routing. For example, there is a problem where the same security routing path may occur by repeated use. This would lead to some nodes with fast energy consumption. It would also shorten the life of the network.

In this paper, we based our model on the iRTEDA protocol [10]. We took the reputation and trust system from the iRTEDA and combined it with the energy of the nodes, the use of a routing selection and the recovery mechanism. Consequently, we were able to obtain a more energy-efficient and reliable security aggregation operation.

3. An Energy-efficient Protocol of Reliable Trust-based Data Aggregation

The ERTDA protocol we developed is based on the RDTA protocol; it also improves the iRTEDA. The basic idea of the ERTDA protocol is on the reputation and trust system. The energy consumption of the nodes combination is reduced. We use the routing path selection

and recovery mechanism to reduce energy consumption to achieve security and a reliable data aggregation in the networks. We introduce the details of the ERTDA protocol as follows:

3.1. Reputation and Trust Computation

In order to improve the estimation accuracy of the reputation value, we observe the regional cooperation between the nodes and exchange each observation in the result list. Each node is based on the results of the observations of all nodes in the region. This is done to better understand the behavior of the node status and estimate the node's reputation and trust values to determine whether the node has compromised nodes.

The ERTDA model is based on the RDAT model. The process of computing the nodes trust value using direct and indirect information is conducted. To accomplish this task, we compute the trust value of the node N_j's data acquisition acts using the node N_i as an example. The trust value calculation of the data fusion and data transmission has the same value as the data collection behavior. $\alpha_{i,j}^{now}$ and $\beta_{i,j}^{now}$ represent the results of a good and bad parameter by the node N_i observation node N_j. Therefore, the new parameters, $\alpha_{i,j}^{new}$ and $\beta_{i,j}^{new}$ [17, 18], are calculated for node N_i as follows:

$$\alpha_{i,j}^{new} = p * \alpha_{i,j}^{now} + m_{i,j} + \sum_{k \in N} R\left(m_{k,j}\right) \tag{7}$$

$$\beta_{i,j}^{new} = p * \beta_{i,j}^{now} + n_{i,j} + \sum_{k \in N} R\left(n_{k,j}\right) \tag{8}$$

where: $m_{i,j}$ and $n_{i,j}$ represent the good and bad qualities of the current data acquisition behavior by node N_i's observation node N_j. At the same time, the information is exchanged between node N_i and N_k *(k=1, 2, ... , n)*. The observed numbers for the correct (good) and bad behaviors are expressed as $R(m_{k,j})$ and $R(n_{k,j})$. *(k=1, 2, ... , n)*, the node N_j's indirect observation information derived from node $N_{i,}$ is [15]:

$$R\left(m_{k,j}\right) = \frac{2 * \alpha_{i,k}^{now} * m_{k,j}}{\left(\beta_{i,k}^{now} + 2\right) * \left(m_{k,j} + n_{k,j} + 2\right) * \left(2 * \alpha_{i,k}^{now}\right)} \tag{9}$$

$$R\left(n_{k,j}\right) = \frac{2 * \beta_{i,k}^{now} * n_{k,j}}{\left(\beta_{i,k}^{now} + 2\right) * \left(m_{k,j} + n_{k,j} + 2\right) * \left(2 * \alpha_{i,k}^{now}\right)} \tag{10}$$

$\alpha_{i,j}^{now}$ and $\beta_{i,j}^{now}$ are the good or bad parameters of the previous observation's results, according to node N_i. The parameters from the previous observations have a considerable influence on the evaluation model, but this influence is less than that of the parameters from the current observation's results. Therefore, we set the attenuation parameter $p<1$, which is weighted. We also obtained $p * \alpha_{i,j}^{now}$ and $p * \beta_{i,j}^{now}$, and combined these values with the current observation results to get the new good and bad parameters, $\alpha_{i,j}^{new}$ and $\beta_{i,j}^{new}$. Subsequently, the Beta model is used to calculate the reputation value $\mathrm{R}_{i,j}^{sensing}$ and the trust value $\mathrm{T}_{i,j}^{sensing}$ of the data acquisition behavior of the node N_j, as follows:

$$\begin{aligned} R_{i,j}^{sensing} &= Beta\left(\alpha_{i,j}^{new} + 1, \beta_{i,j}^{new} + 1\right) \\ &= \frac{\Gamma\left(\alpha_{i,j}^{new} + 1 + \beta_{i,j}^{new} + 1\right)}{\Gamma\left(\alpha_{i,j}^{new} + 1\right) \cdot \Gamma\left(\beta_{i,j}^{new} + 1\right)} \varphi^{\left(\alpha_{i,j}^{new} + 1\right) - 1} \left(1 - \varphi\right)^{\left(\beta_{i,j}^{new} + 1\right) - 1} \end{aligned} \tag{11}$$

$$T_{i,j}^{sensing} = E\left(R_{i,j}^{sensing}\right) = \frac{\alpha_{i,j}^{new} + 1}{\alpha_{i,j}^{new} + \beta_{i,j}^{new} + 2} \tag{12}$$

The network, according to the observation results of node N_i, calculated the data acquisition behaviors' trust value for node N_j to determine whether the node N_j was compromised. Once the trust value exceeded the preset threshold value, the decision became that the node N_j was not to be trusted; as such, it was excluded from the network. As described previously, the data aggregation and transmission behavior of the nodes use the same method to calculate the trust value of the node behaviors that monitor and judge whether the node is a trusted node.

3.2. Energy and Link Availability

The trust management mechanism can be used to ensure there is security in data collection, data fusion and data forwarding in the wireless sensor nodes. It can also be used to detect a mutual trust relationship and communication security between the nodes to exclude the compromised nodes from the network and avoid the negative impact of the compromised nodes forgery detection data. However, only depending on the trust management mechanism means you are unable to monitor and ensure that a node has enough energy to undertake and complete the tasks in a reliable way. Consequently, when we select the aggregation nodes and forwarding nodes, they must integrate the node's residual energy and trust management mechanism together, so we are better able to judge the results. If it is only based on the trust management mechanism, there will be a higher level of trust value aggregation nodes and paths repeatedly used. There will also be a relatively low trust value of the nodes and the path will be used less, resulting in the excessive use of node energy and the energy use will be unbalanced; this would decrease the entire network's life cycle.

In order to improve the reliability of data aggregation and energy efficiency, the nodes need to detect both the behavior of the neighbor node, the assessment around the node's reputation and trust value, and the nodal energy. When exchanging messages, the node's residual energy and behavioral observations results are broadcasted to the neighbor nodes. This can be used to integrate the energy and the parameters of the trust value calculations. It can also be used to obtain the link between the availability of the nodes. In this way, we can play three roles:

(1). Each cluster of aggregation nodes needs to have their security ensured. They also need to have enough energy for the aggregation operation and data forwarding. When choosing the aggregation nodes, we must also consider the two elements of the trust value and energy to achieve the trust value and energy balance.

(2). The link availability is calculated according to the energy of the neighboring nodes. It illustrates the reliability of the data transmission link between the nodes to ensure that there is enough energy for transmission between the nodes.

(3). The results of the data-aggregation process are necessary to select multiple paths to the base station, as the data communication process needs sufficient energy. When selecting a transmission path, we need combine the trust value of the node and the link availability together to ensure the reliability of the transmission path and choose a better transmission path.

N_{ET} represents the comprehensive parameter of the trust value and the energy value. The energy value is introduced into the trust value, which is used to determine the new aggregation node and the forwarding node in the transmission path. However, in the iRTEDA model, the N_{ET} excessive dependence on the energy parameters, N_{ET} , can appear as negative

values, while the trust value increases; that affects the model simulation a lot. As such, we redefine N_{ET} in the ERTDA model as:

$$N_{ET} = \frac{E}{E_{Init}\text{-}E} \cdot \left(\sum_{k=1}^{k} \frac{E_k}{E_{Init}\text{-}E_k} \right) \cdot T$$
$$E > \theta_{Eg}^{Ag}, T > \theta_{T}^{Ag} \tag{13}$$

where: E represents the energy of the node, T represents the trust values of the node, E_k represents the node's energy on the aggregation path of the remaining k nodes, E_{Init} and T_{Init} represent the initial energy and the initial trust value of the node, respectively, and $\theta_{Eg}^{Ag}, \theta_{T}^{Ag}$ represent the minimum acceptable energy value and trust value of the node, respectively. When the value of N_{ET} is large, the aggregation node becomes stronger and more reliable. In addition, the trust value and energy value are then able to undertake the work of the aggregation node.

L_{AB} represents a link availability between Node A and Node B:

$$L_{AB} = \frac{(T_{\text{init}} - T_{AB}) \cdot (\text{E}_{init} - E_B)}{T_{AB} \cdot E_B}$$
$$E_B > \theta_{Eg}^{relay-node}, T_{AB} > \theta_{T}^{link} \tag{14}$$

where: T_{AB} represents the trust value assessment from Node B to Node A, E_B represents the residual energy of Node B, $\theta_{Eg}^{relay-node}$ and θ_{T}^{Link} represent the minimum energy and the minimum trust value of Node B's forwarding required data, respectively.

Two nodes, *i* and *j*, are on the transmission path. The *p* intermediate nodes link with Node *i* and Node *j*, expressed as s_l *(1<l<p)*. The parameter *L(i,j)* represents an availability link between Node *i* and Node *j*. The availability of all of the links between the nodes *i* and *j* is represented by *Link(i,j)* and expressed as:

$$Link(i,j) = L(i,j) + \sum_{l=1}^{p} \min\left(L(i,s_l), L(s_l,j)\right) \tag{15}$$

Parameter *Link(i, j)* is used to evaluate the link availability between Node *i* and Node *j*, to ensure that the selection process of the chosen nodes can be more reliable and have a more adequate amount of energy.

In addition, set *U(i)* represents the links set from Node *i* to the neighbor Node s_l *(1<l<p)*. The set *U(i)* represents the neighbor nodes, which are the intermediate nodes from the Node *i* to the Node *j*. The Node *i* will be assigned the weights of the neighbor nodes in set *U(i)*. The Node s_l is the intermediate node on the link from the Node *i* to the Node *j*; it belongs to the set *U(i)*. *Link(i, s_l)* represents the link availability from the Node *i* to the Node s_l. w_j represents the link reliability weights from the Node *i* to the Node s_l:

$$w_j = \frac{Link(i,j)^{\alpha}}{\sum_{m \in U(i)} Link(i,m)^{\alpha}} \tag{16}$$

When $\alpha = 0$, Node i, in relation to all the neighbor nodes', has a link of *U(i)*, where all have the same priority, in accordance with the link reliability select data transmission link. When $\alpha > 0$, the higher the link reliability in the set U (i), the greater the weight w_j; this becomes the higher priority aspect of the data transmission link. When α tends to infinity, we select the highest link reliability node as the routing forwarding node.

Therefore, when Node *i* chooses a safe and reliable link to the base station, we use the link's reliability of Node *i* to the neighbor node set *U(i)* to determine whether Node *i*'s neighbor nodes become becoming a forwarding node is sufficiently reliable. If we need to choose more security and better energy balance data forwarding nodes, we set parameter $\alpha = 0$, $\alpha = 0$; this makes the link weight w_j of . The node to the neighbor node will be set for Node i to connect the neighbor node. In order to simplify the analysis in the trust management model, in this paper, we set the parameters $\alpha = 0$ and weight $w_j = 1$.

3.3. Recovery Mechanism

The monitoring node is based on the direct and indirect information obtained by the target nodes to calculate the target node's trust value. As such, the calculated trust value is uploaded to the aggregation node. The aggregation nodes, according to the trust value of the target node, are used to determine whether these nodes are compromised nodes. Once a node is determined as a malicious node or a compromised node, by the aggregation node, that aggregation node will broadcast the message to notify all of the nodes in the surrounding area. This will result in the compromised node being excluded from the communication network. This node's data and routing are not within the choice of the network.

The emergence of the compromised nodes will inevitably lead to the corresponding child nodes possibly becoming the isolated nodes. As such, the recovery mechanism can be detected in the compromised nodes, reducing the possibility of the isolated nodes in a network. The nodes in the WSN have a cluster structure to organize themselves. Each cluster head consists of an aggregation node, data collection and a fusion operation. When a compromised node appears, depending on the different types of compromised nodes, it is divided into different situations to repair the network: (1) the leaf node is compromised; (2) the intermediate node is compromised; (3) the aggregation node is compromised; and (4) the node in the routing path is compromised. In order to more obviously compare the simulation data, in this paper, we use the same recovery mechanism as in the iRTEDA protocol [10].

4. Performance Evaluation

To evaluate the performance of the ERTDA model, we compared the data-aggregation operations based on the ERTDA model and the iRTEDA model with the average trust value, the accuracy of the polymerization, the energy consumption, the life cycle and the nodal mortality. We used the Tiny OS 2.0 simulator (TOSSIM) and its variant, PowerTOSSIM, a power modeling extension to TOSSIM to conduct the simulations. PowerTOSSIM accurately models power consumed by TinyOS applications. One hundred sensor nodes were deployed in the network that had an area of 300 m $\times$ 300 m; they were organized according to the cluster structure. The base station deployed in the regional center, the cluster head node, was used as the polymerization node. There were a certain proportion of compromised nodes in the network, which sent the wrong data to the aggregation node. We set the connection between the node failure and packets loss as a fixed ratio.

4.1. Comparison of the Reputation Value

To evaluate the effectiveness of the ERTDA trust management model, we used a statistical method to calculate the average reputation values for a period of running time within the network. 30% of the nodes existing in the network were compromised; all of these compromised nodes exhibited error behavior in the data collection, transmitting and aggregation process. The monitoring nodes observed the error behaviors of the compromised

nodes, recorded the good and bad numbers of the observed behaviors, and computed the reputation value and the trust value of the nodes. The ERTDA model, in view of the three nodes' behaviors, calculated the reputation value and the trust value, this included: the reputation value of the node data-collection $R_{i,j}^{sensing}$, the reputation value of the node data-aggregation $R_{i,j}^{aggregating}$ and the reputation value of the node date- transmission $R_{i,j}^{routing}$.

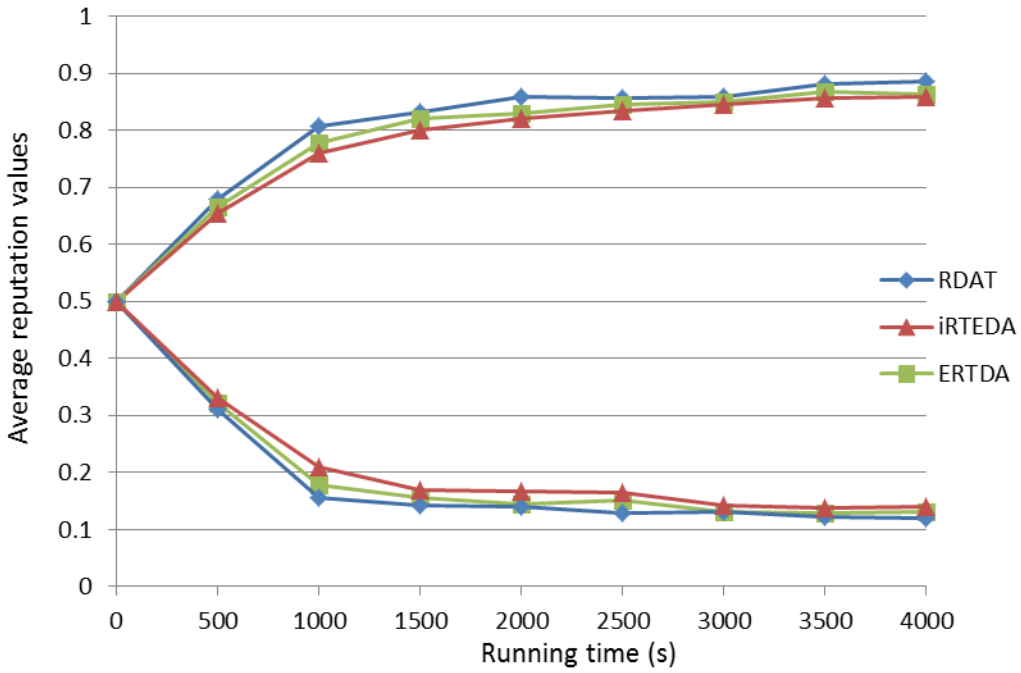

Figure 1. Comparison of the Average Reputation Values

Figure 1 compared the changes in the average reputation values of the three models. According to the Beta model, in the beginning of the networks, the good behavior number was the same as the bad behavior; the starting point of the reputation value is 0.5. With the operation of the network, the reputation values changed in both directions. The average reputation values of the legitimate node increased gradually. In the running of the first 1000 seconds, the average reputation values of the legitimate node increased at a faster rate. The average reputation values of the 1000 seconds reached a higher value. The average reputation values of the legitimate node, based on the ERTDA model, were slightly less than that of the RDTA model and slightly higher than that of the iRTEDA model. The reason for this is that the nodes of the ERTDA considered the trust value of each node, the remaining energy of the nodes and the connection of the nodes. This resulted in a reduction in the overall security of the networks, an improvement in the energy consumption, and an improvement in the stability and reliability of the networks. However, the extent of the decline in the average reputation values was small; this would not have much of an impact on the detection of the compromised node.

4.2. Comparison of Data-Aggregation

Aggregation accuracy is an important evaluation index of a security data-aggregation technology in WSN. Aggregation accuracy is defined as the amount of data from the legitimate aggregation nodes in terms of the ratio of the base station's collected data. When

the ordinary node is compromised, the data collected by these nodes will belong to the illegal data. If the aggregation nodes that manage the ordinary nodes have been found to be compromised nodes, this data will be abandoned and not adopted. However, if the aggregation nodes are compromised, the collection and uploaded data from the aggregation nodes will be used for the data-aggregation. Consequently, the aggregate results set will be illegal and the data cannot be trusted.

Figure 2 compared the changes in the aggregation accuracy of the three models. As can be seen from Figure 2, the three models growing trend in aggregation accuracy was the same, but the growth rate was significantly different. At the beginning of the network operation, the aggregation accuracy of the ERTDA model was less than that of the other two models, because the ERTDA model introduced the energy parameters and the routing link into the trust management mechanism. In this way, the nodes of the network were monitored and the trust value was not entirely considered. As the extension of the network running time, the nodes energy in the higher trust values of the iRTEDA model and the RDAT model was gradual consumption; only the nodes with low trust values could be used for data transmission. Since the parameters setting of the nodes energy were effective in the ERTDA model, the results of the nodes energy consumption was more balanced in the model, and thus, higher trust value nodes were reserved. The growth rate of the ERTDA model's aggregation accuracy was greater here than in the other two models'. The ERTDA model also introduced the energy parameters and the routing link to improve the aggregation accuracy. As such, the recovery mechanism reduced the number of isolated nodes, increased the number of legitimate nodes, and improved the aggregation accuracy.

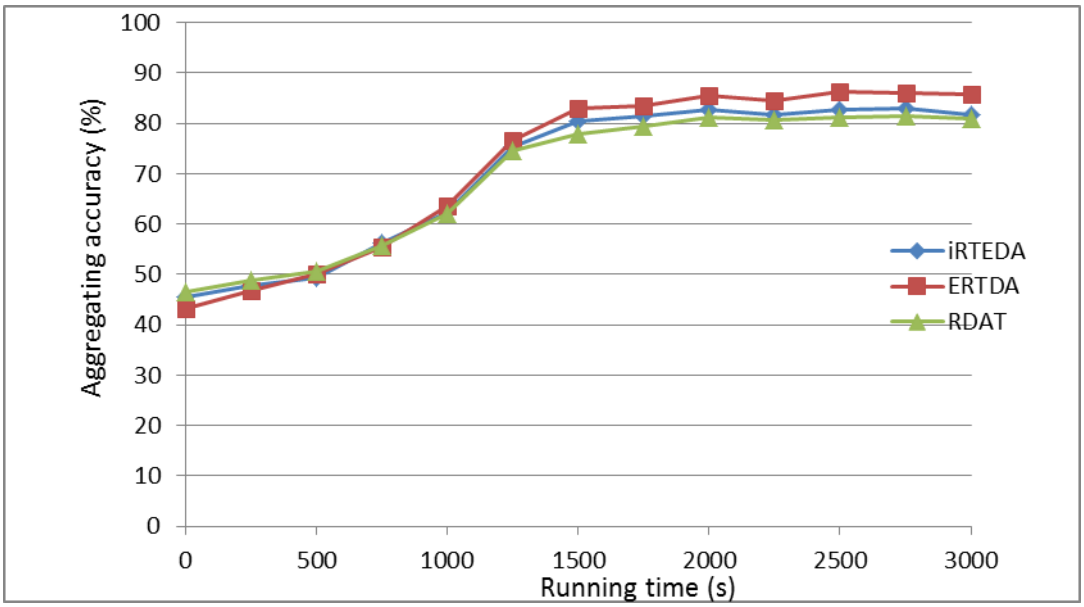

Figure 2. Comparison of the Aggregating Accuracy

4.3. Comparison of the Energy Consumption

Life was one of the key elements used to evaluate the good or bad performance of the WSN. The number of dead nodes in the three models was compared to determine the performance of the three trust management model. The higher death rate of the nodes show that if there are more nodes failing, the performance will be worse and there will be a higher level of energy consumption in the network.

Figure 3 compared the changes in the number of dead nodes in the three models. We observed that the death rate of the nodes in the three networks presented entirely different trends. Along with the network operation, in the network based on the RDAT model, the death rate of the nodes was much higher than that of the other two networks. The reason for this is that the network based on the RDAT protocol selected the forwarding nodes without considering energy consumption. It only considered the trust values of the nodes, resulting in the selective forwarding nodes having high trust values. Consequently, the nodes with higher trust values in the process of the data transmission were excessive used; this caused a large number of the nodes to use too much energy, resulting in an excessive number of dead nodes. The rationality of the parameter setting in the ERTDA protocol also made the death rate of the nodes in the network based on ERTDA model lower than of the iRTEDA model. When the network was run for 2500 seconds, the network RDAT model left the nodes of lower trust values and isolated nodes; the death rate of the nodes also began in a low state. At the same time, the energy consumption of the nodes based on the ERTDA model had a good balance; the situation with the higher trust value and excessive energy consumption did not occur. After the network ran for 2500 seconds, the death rate of the nodes in the network based on the ERTDA model appeared to increase. This is due to many nodes at this time having already consumed a lot of energy. This resulted in the continued operation of the network causing the nodes with little energy to fail.

Figure 4 compared the changes in the energy consumption of the three networks. When the network operation ran for 2500 seconds, the energy consumption of the network based on the ERTDA model was 40.6%; this value was far less than the 44.3% of the RDAT model and the 44.3% of the iREDAT model. The reason for this is that, along with the network operation, the compromised nodes and low trust value nodes were constantly monitored by the trust management mechanism and excluded from the scope of the network; this improved the network security as a whole. However, while the security threats in the network were eliminated, some nodes had connections with compromised nodes; these nodes became isolated nodes. The ERTDA model introduced a repair mechanism to help these isolated nodes, making them re-select a parent node and rejoin the cluster structure. This reduced the communication overhead of these nodes. Therefore, the ERTDA model was more conducive to reducing the energy consumption of the network and extending the life of the network.

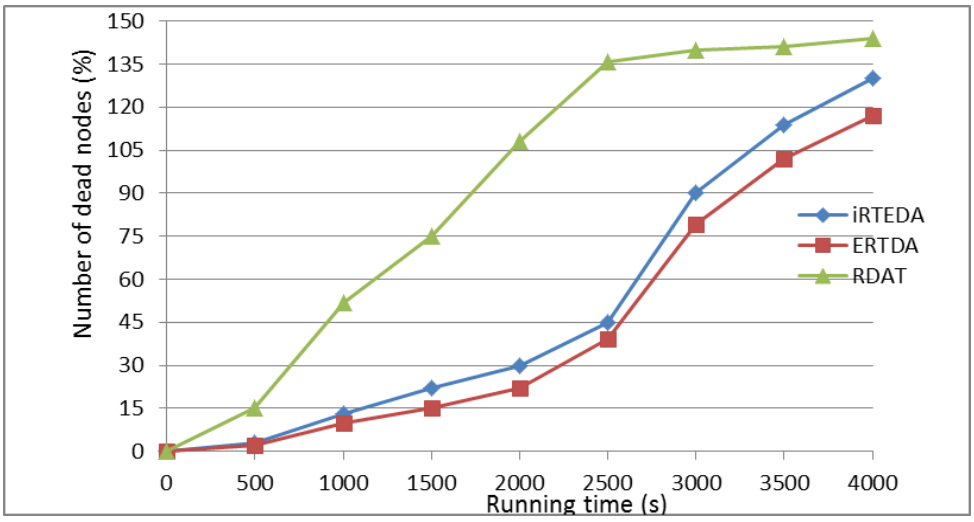

Figure 3. Comparison of the Number of Dead Nodes

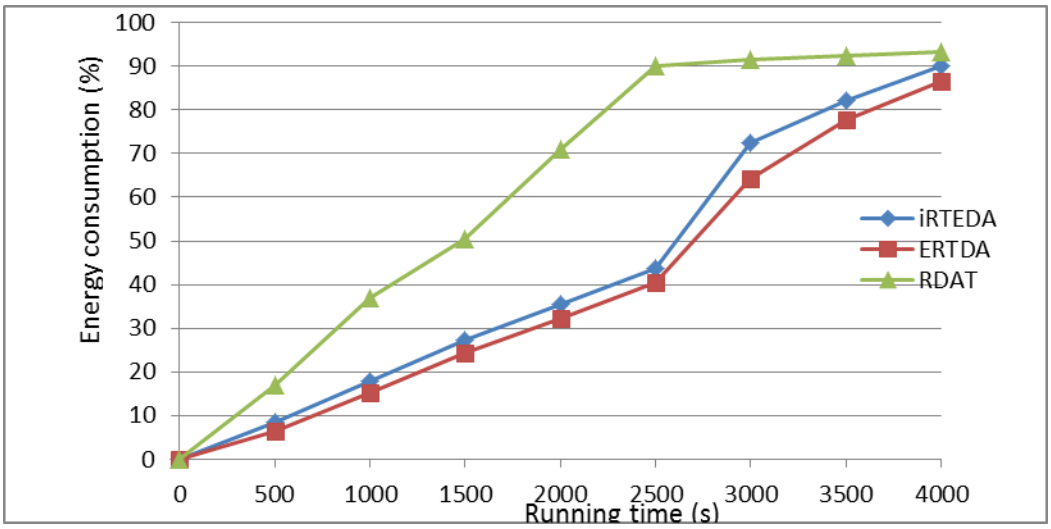

Figure 4. Comparison of the Energy Consumption

5. Conclusions

In this paper, we presented an energy-efficient protocol of a reliable trust-based data aggregation for WSN. The ERTDA protocol can replace the RDAT algorithm, which only considers the node trust value, rather than the defects in the node energy and the availability routing link. As such, the ERTDA protocol improves the excessive dependence on the energy parameters of iRTEDA protocol.

The ERTDA protocol calculates the trust values of nodes, monitors and evaluates the nodal trust degree, and timely detects and excludes the compromised nodes based on the observation of the nodal behavior. The simulation results illustrate that the ERTDA protocol can improve the accuracy of an aggregation effectively. It can also reduce the mortality rate and the energy consumption of a node, improve the reliability of data transmission and extend the effective life of the networks.

References

[1] D. Culler, D. Estrin and M. Srivastava, "Computer", vol. 37, no. 41, **(2004)**.
[2] K. Römer, "Programming Paradigms and Middleware for Sensor Networks", Proceedings of GI/ITG Workshop on Sensor Networks, **(2004),** Karlsruhe, Germany.
[3] J. Yick, B. Mukherjee and D. Ghosal, "Comput. Netw.", vol. 52, no. 2292**, (2008)**.
[4] B. Ishnamachari, D. Estrin and S. Wicker, "Impact of data aggregation in wireless sensor networks", Proceedings of the 22nd International Conference on Distributed Computing Systems, Vienna, New York **(2002).**
[5] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks [J]", Communications of the ACM, **(2004),** pp. 53-57.
[6] J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: Analysis and Defenses [C]", In Proceedings of IPTPS, New York, ACM Press, **(2002)**, pp. 259-268.
[7] C. Karlof and D. Wagner, "Secure routing in sensor networks: Attacks and countermeasures [V]", Ad Hoc Networks, **(2003)**, pp. 293-315.
[8] S. Ozdemir, "Functional Reputation Based Data Aggregation for Wireless Sensor Networks [C]", IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, Avignon, IEEE Press, **(2008)**, pp. 592 – 597.
[9] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks [J]", Computer Communications, vol. 31, no. 17, **(2008)**, pp. 3941–3953.

[10] C. Liu, Y. Liu and Z. Zhang, "Improved Reliable Trust-Based and Energy-Efficient Data Aggregation for Wireless Sensor Networks [J]", International Journal of Distributed Sensor Networks, **(2013)**.
[11] L. Mui, M. Mohtashemi and A. Halberstadt, "A computational model of trust and reputation for e-businesses [C]", In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02), Washington DC, USA, IEEE Press, vol. 7, **(2002)**, p. 188.
[12] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities [C]", In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS'00), Hawaii, USA, ACM Press, vol. 6, **(2000)**, pp. 1-9.
[13] P. Dasgupta, "Trust as a commodity", Trust: Making and Breaking Cooperative Relations, **(2000)**, pp. 49-72.
[14] A. Jsang, R. Ismail and C. Boyd , "A Survey of Trust and Reputation system for online service provision [C]", Decision Support System, **(2005),** pp. 618-644.
[15] S. Ganeriwal, L K. Balzano and M. Srivastava, "Reputation based framework for high integrity sensor networks [C]", ACM Transactions on Sensor Networks, vol. 4, no. 3, **(2008)**, pp. 1–37.
[16] I. Josang, "The beta reputation system [C]", the 15th Bled Conference on Electronic Commerce, **(2002)**, p. 41.
[17] S. Ozdemir, "Functional Reputation Based Data Aggregation for Wireless Sensor Networks [C]", IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, Avignon, IEEE Press, **(2008)**, pp. 592 – 597.
[18] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks [J]", Computer Communications, vol. 31, no. 17, **(2008)**, pp. 3941–3953.