A distributed data secure transmission scheme in wireless sensor network

Wei Liang, Yin Huang, Jianbo Xu and Songyou Xie

Abstract
Sensor nodes around monitoring area have various distances to the target node. Therefore, it is difficult to ensure security of broadcasting data transferred from a single wireless sensor node to base station. Multi-hop transmission of data between sensor nodes wastes network resource. In this case, a distributed data secure transmission scheme is proposed in a wireless sensor network. Data transmission is classified into two stages: constructing a collection of receiving nodes and selecting a unique forwarding node from this collection. These are implemented using analysis of relative movement distance between nodes and transfer time competitive mechanism. Besides, we have assumed a network model for distributed data secure transmission to improve efficiency of data transfer. This design includes secure model of node competition, data perception model, and anti-resistance model. Moreover, the security of competition transfer for nodes in wireless sensor network is evaluated. Finally, simulation proves that the proposed scheme has good performance in security and stability compared to similar schemes.

Keywords
Wireless sensor network, distributed data, distributed data secure transmission, data perception model, security evaluation

Date received: 14 December 2016; accepted: 23 March 2017

Introduction
Wireless sensor network (WSN) is widely applied in many fields, such as military battlefield, disaster rescue, environment monitoring, traffic management, trail report, and medical care. As shown in Figure 1, WSN consists of mobile sensor nodes and sink node. Sensor node is deployed on mobile entity for collecting necessary information. Sink node can be fixed or mobile for receiving information from sensor nodes and transmitting it to backbone network. Different with traditional network, this network has features such as rapid mobility of nodes, dynamical network topology, and requirement of high security and reliability.

(1) **Limited power capacity.** Sensor nodes are battery-powered. But battery capacity always has limited energy. Besides, sensor nodes are generally deployed in severe environments like desert and battlefield. The number of nodes is always large. It is not practical to change battery or charge battery to prolong network lifetime. So, low energy consumption is first considered in any technique and protocol to prolong network lifetime in designing a sensor network.

(2) **Dynamic topology.** WSN is a dynamic network. The topology structure changes under the following conditions: (1) node invalidity caused by energy, environment, and so on; (2) addition of new node; and (3) mobile node in...
network. Consequently, WSN can reconstruct network dynamically.

### (3) Data centered

Traditional network is connection centered, but WSN is data centered. When WSN reports monitoring events or users inquire events with WSN, only events concerned by WSN are reported to users, not concerning the event from which sensor node. This feature makes WSN a data-centered network.

### (4) Limited computation ability

Nodes in WSN have weaker processor owing to limited volume and power. Complex computation and data storage cannot be realized by these nodes. So, simple algorithm is required in WSN, which can be easily implemented in the sensor node.

### (5) Self-organization

Sensor nodes are always deployed by aircraft. So, positions and adjacency relationship of these nodes cannot be determined in advance. Besides, sensor network has dynamic topology. Self-organization is required for automatic configuration and management. Multiple-hop wireless network is automatically constructed by topology-control mechanism and network protocol.

### (6) Wide distribution and large scale

Sensor nodes are always deployed in a wide area, especially in severe environment without human race. Network maintenance is much difficult. To obtain reliable and precious information, large number of sensor nodes will be deployed in the monitoring area. It reduces or eliminates monitoring dead zone caused by node validity. The performance of fault tolerance is enhanced.

Nodes in WSN have high energy consumption and low success rate of data transmission. We analyze previous data transmission protocol and propose a distributed data secure transmission (DDST) protocol in WSN. DDST divides data transmission into two stages, namely, constructing a collection of receiving nodes and selecting a unique forwarding node from this collection. DDST uses relative movement analysis and competitive mechanism based on forwarding time. This protocol has the following features: (1) receiver-based data transmission. Generally, sender-based data transmission needs to create global routing from source node to sink node. This global routing is not necessary in receiver-based data transmission. A proper candidate node is selected in neighboring nodes of sending node for receiving data. (2) Success rate of data transmission. This article has set two conditions. First, candidate node will not move out of the communication range in data transmission period. Second, candidate node should be set within the intersection of communication area and the 60-degree-sector-oriented sink node. The candidate should satisfy both conditions. (3) Competitive mechanism based on forwarding time. This mechanism is applied in selection of forwarding node. It forwards data instead of multiple nodes. In this case, the number of communication nodes and energy consumption are reduced. (4) Secure data forwarding protocol. The protocol weeds out candidate receiving nodes continuously, changing it from working state to dormant state to save energy. In addition, the forwarding time-based competitive mechanism selects the forwarding node with the most energy. The simulation proves DDST can effectively prolong network lifetime and achieve better data transmission rate.

This article is organized as follows. The second part gives an overview of related work. The DDST protocol is introduced in the third section. After that, the implementation of DDST is concretely illustrated. The fifth section analyzes and compares the experimental results. Finally, this work is concluded.

### Related work

WSN is designed to sense and acquire information in objective physical world. Data transmission protocol is the foundation of various applications in mobile sensor network (MSN) and should be considered in network construction. To design a data transmission protocol, one should consider not only energy consumption of each node but also network lifetime.

Mobile WSN has different application fields, which requires various transmission protocols. On this basis, data transmission protocol in WSN can be classified into four categories, namely, transmission protocols based on replication, clustering, quality of service, and geographic information. Geographic information-based data transmission protocol is widely used. Node position has large impact on data transmission. In network service, the sensing data of nodes is meaningful only after the geographic information is obtained.
Recently, researchers conducted much work on static WSN because the mobility of nodes in mobile WSN will change network topology, interrupt, or invalidate the routing path. So, many data transmission protocols in WSN cannot be applied to MSN.

Some clustering-based data transmission protocols are proposed in MSN. The famous low-energy adaptive clustering hierarchy (LEACH) protocol assumes nodes are static. When these nodes move, LEACH loses lots of data. It proves the protocol is not suitable for MSN. DS Kim and YJ Chung proposed low-energy adaptive clustering hierarchy–mobile (LEACH-M) protocol by improving LEACH to support mobile nodes. In each transmission, an acknowledge message is sent to cluster head to confirm whether a mobile node can communicate with cluster head. Compared to LEACH, LEACH-M obviously improves data transmission success rate. However, LEACH-M selects cluster head with random probability, which is the same with LEACH. The mobility of cluster head is not considered. If the cluster head moves out of its cluster before cluster head rotation, the cluster will be broken, causing lots of packet loss.

Replication-based transmission protocol is that multiple data copies will be transmitted to improve data transmission success rate. Wang and Wu proposed a message fault tolerance-based adaptive data delivery scheme (FAD). The computation of data transmission rate is the same with that of replication-based efficient data delivery scheme (RED). Queue is managed using fault tolerance value. When the queue is full and queue message updates, some messages with the fault tolerance value greater than the threshold value will be dropped. FAD is an improvement of RED, which has better data transmission rate. But the energy consumption is higher than that of RED. Li et al. proposed a receiver-based cross-layer forwarding (RCF) protocol. The protocol utilizes a self-adaptive mechanism for forwarding right contention. Also, it deals with the data collision and multi-cast suppression better through the dual-channel communication model and puts forward an efficient routing void bypass mechanism. RCF has good reliability, but dual-channel communication consumes more energy. Lu and Li proposed a novel probability distribution-based dynamic and predicted (PDDP) data forward strategy. It utilizes mobility of sensor nodes to create dynamic path which can achieve a network delay close to optimum value, at the same time, consume network resource efficiently. This strategy has high robustness and practicality. The geographic information-based data transmission protocol can be classified into two categories: sender-based protocol and receiver-based protocol. Wang and Wu presented an RED. It utilizes history data-based forwarding method to compute transmission rate and introduces erasure coding to improve efficiency. This protocol has balanced transmission efficiency and overhead. The used theory is simple but effective. High transmission efficiency is achieved. Blum et al. proposed an implicit geographic transfer protocol. The forwarding area is limited within a sector of 60°. Waiting time of sender node is set on basis of the distance between receiver node and sink node and its remaining energy. It has solved the problem of multi-cast inhibition and considered energy.

**DDST protocol**

**Network model**

Data transmission protocol in MSN is studied in this article. The network model should satisfy four conditions as follows:

1. Assume that \( N \) sensor nodes with communication radius \( r \) are randomly deployed in a monitoring area \( Q \), as shown in Figure 2. After being deployed, these nodes can move with a slow speed and each has a unique ID, namely, \( 1, 2, ..., n \). The ID of sink node is set as 0. Sink node cannot move and other nodes are randomly deployed with high density to ensure connectivity of this network.

2. Each wireless sensor node can sense its remaining energy in real time. Initial energy of each node could be different and not be added. This case is more close to real network.

3. Each node in WSN carries a module-like global positioning system (GPS). So, the information such as position, movement speed, and direction could be sensed by itself.

4. The time of all nodes in WSN is synchronized. Data are transmitted by cooperation to avoid collision and save energy.

![Figure 2. Network model of DDST protocol.](image-url)
**DDST protocol analysis**

This section gives some important definitions before analyzing DDST protocol:

Definition 1: Communication circle. A node in MSN moves at any time. The area, used the node as the center to form a circle with communication radius, is called communication circle.

Definition 2: Node density. The number of nodes in unit area at any time is node density, denoted by “ρ.”

Definition 3: Data transmission success rate. During a communication period of MSN, the ratio of data amount received by sink node to data amount sent by sending node is data transmission success rate.

In this article, a DDST protocol is proposed in WSN. DDST divides data transmission into two stages, namely, constructing a collection of receiving nodes and selecting a unique forwarding node from this collection. DDST uses relative movement analysis and competitive mechanism based on forwarding time. This protocol achieves effective, rapid, and precious data transmission.

The first stage is to construct a collection of receiving nodes. A unique forwarding node is selected from this collection. This article has set two conditions for candidates. First, candidate node will not move out of the communication range in data transmission period. Second, candidate node should be set within the intersection of communication area and the 60-degree-sector-oriented sink node. The candidates should satisfy both conditions. It reduces data receiving and the speed, which is energy saving.

It is unnecessary for every node to receive data. After constructing the collection of candidates, the second stage starts. This stage selects a unique forwarding node from the collection of candidates. The competitive mechanism based on forwarding time is used in this stage. We introduce this mechanism as follows. After receiving data, the mechanism will compute forwarding competitive time of each candidate, \( t = (k \times d \times T) / E_r \).

Here, the parameters \( E_r \), \( d \), \( T \), and \( k \) are, respectively, remaining energy, distance to sink node, communication period, and regulation parameter. The parameter \( k \) makes it satisfy \( 0 < (k \times d) / E_r < 1 \). The node with the minimum forwarding competitive time is selected as data forwarding node. From the expression to compute \( t \), more remaining energy and short distance to sink node make \( t \) the minimum.

**Description of DDST protocol**

In DDST protocol, data transmission has six cases, as shown in Figure 3. Wireless sensor node is denoted by small yellow circle. Assume the node of ID 1 is the sending node with original perception data. The communication radius is \( R \). The circle with the center of node 1 and radius of \( R \) is called communication range. Node 1 is used to send data. Nodes with ID 11, 12, 13, and 14 exceed the communication radius of node 1, which cannot receive data. They can do nothing but sleep. The nodes with ID of 6, 7, 8, 9, and 10 are within the communication area. They can receive data from node 1, but cannot be added to collection of candidates because they are far away from sink node and cannot satisfy the second condition. Nodes with ID 3, 5, 15, and 16 are within the communication area, which can receive data and satisfy the second condition. But the first condition is not satisfied. So, these nodes cannot be candidates. Node 4 satisfies both conditions, which will be added in collection of candidates. But the forwarding competitive time is long, so it cannot be selected as forwarding node. Only node 2 satisfies both conditions and has shorter forwarding competitive time. It is selected as unique forwarding node.

DDST is described as follows. At the stage to collect receiving nodes, communication is unnecessary. When the source node wants to send data, other nodes will compute collection of candidates based on algorithm of receiving nodes. The candidates receive data packages from source node. It achieves high data-reception rate with lower energy consumption. As shown in Figure 3, the sending node 1 broadcasts its location. Nodes with ID from 2 to 16 can receive the information, but nodes from 11 to 14 are out of communication area. The nodes satisfying both conditions above are suitable for data transmission. From Figure 3, node 2 and node 4 receive data package.

After that, we use competitive mechanism in collection of receiving nodes to determine node time. First, a time interval \( t \) is set. Each candidate automatically performs forwarding competitive mechanism to compute the forwarding competitive time. The node with the
minimum time is selected as the forwarding node. As shown in Figure 3, the candidates are node 2 and node 4. They locate within the communication area of sending node. When they receive data from node 1, the forwarding competitive time is computed. Node 2 has short forwarding time, so it is selected as forwarding node. Node 4 drops the data package and sleep. After that, node 2 becomes sending node, repeat above procedures until the data package from node 1 has been sent to sink node.

**Construction of candidates nodes.** The main task of first stage is to select candidates from neighboring nodes of sending node. The neighboring nodes analyze their information and determine whether they satisfy the following two conditions:

**Condition 1.** Candidate node will not move out of the communication range in data transmission period.

**Condition 2.** Candidate node should be set within the intersection of communication area and the 60-degree-sector-oriented sink node.

The candidates should satisfy both conditions. For condition 1, nodes which will not move out of communication area during period of data sending can be added to candidate collection. The nodes are mobile, so relative motion analysis between nodes is required to judge whether it will move out of communication range during a period. It lays foundation for the second stage. Only those nodes satisfying conditions can become receiving nodes. Otherwise, nodes go to sleep.

The communication period $T$ of a node is short, and node movement is regarded as uniform linear motion. We focus on the motion of receiving node to analyze the relative motion between nodes. The details are illustrated as follows.

The main parameters are set as follows. Assume that the movement speed of sending node is $v_1$ and candidate moves with speed of $v_2$. The angle between motion direction of sending node and receiving node is denoted as $\alpha$. The angle between motion direction of receiving node and sending node is denoted as $\beta$. The communication radius is $R$. $d$ and $r$ are distances from sending node to candidate node and communication period, respectively.

In Figure 4, node S is the sender and N is a neighboring candidate of S. After a period, we need to analyze whether N will move out of communication area of the sender. After time $T$, S moves to E and N moves to M. Now, we compute $d'$, namely, the value of $||\text{ME}||$. $d' < R$ demonstrates that N will not move out of communication area after time $T$. The first condition is satisfied and it can be selected as data receiving node.

As shown in Figure 4, in the direction parallel to connection of two nodes, relative displacement $||OM||$ could be computed when the value of $\beta$ is different.

When $\beta$ is between $0^\circ$ and $90^\circ$, or between $270^\circ$ and $360^\circ$

$$|OM| = d - v_1 * T * \cos \alpha - v_2 * T * \cos \beta$$

$$= d - (v_1 * \cos \alpha + v_2 * \cos \beta) * T$$

(1)

When $\beta$ is between $90^\circ$ and $270^\circ$

$$|OM| = d - v_1 * T * \cos \alpha + v_2 * T * \cos \beta$$

$$= d - (v_1 * \cos \alpha - v_2 * \cos \beta) * T$$

(2)

In the direction vertical to connection of two nodes, the relative displacement is computed as follows.

When $\beta$ is between $0^\circ$ and $180^\circ$

$$|OE| = v_1 * T * \sin \alpha + v_2 * T * \sin \beta$$

$$= (v_1 * \sin \alpha + v_2 * \sin \beta) * T$$

(3)

When $\beta$ is between $180^\circ$ and $360^\circ$

$$|OE| = v_1 * T * \sin \alpha - v_2 * T * \sin \beta$$

$$= (v_1 * \sin \alpha - v_2 * \sin \beta) * T$$

(4)

After time $T$, the distance $d'$ between two nodes could be computed through equations (1)–(4)

$$d' = \sqrt{|OE|^2 + |OM|^2}$$

(5)

By comparing $d'$ to $R$, we can determine which node will be data receiving node. If $d' < R$, the first condition to be forwarding node is satisfied. Otherwise, it cannot be the forwarding node. Candidate node should be set within the intersection of communication area and the
60-degree-sector-oriented sink node as shown in Figure 5.

In Figure 5, S is sending node, R is communication radius (m) of S. S has many neighboring nodes. Among these nodes, A, B, C, D, E, and F can be regarded as candidates. Although H, I, J, and K are within communication area, they are not in the interaction area of communication area and the 60-degree-sector-oriented sink node. So, they cannot be added to the collection of candidates. Other nodes can satisfy the second condition of candidates.

Selection a unique forwarding node from candidate nodes. In this section, the forwarding node will be selected from the candidates using competitive mechanism, namely, forwarding-based competitive mechanism. After receiving nodes receive data, the competition for data forwarding starts. Sensor nodes could be aware of its information. So, it can compute the forwarding competitive time. After that, each receiving node detects the busy signal. If there is no busy signal when its forwarding competitive time comes, the node will send a data package to sending node and tell that it can forward data. When the sending node receives package, inhibition package is generated to stop sending other request packages. If busy signal is detected, the received data will be dropped. As known, the receiving node with the minimum forwarding competitive time has superiority of information interaction with sending node. It successfully becomes the node to forward data.

Two parameters are required to compute forwarding competitive time: remaining energy \( E_r \) and distance to sink node \( d \). \( T \) is communication period and \( \lambda \) is weight value

\[
Time = \lambda \frac{d}{E_r} \frac{T}{C_3}
\] (6)

The consideration of energy and distance to sink node is to balance energy consumption and reduce hops of data forwarding. From equation (6), the forwarding competitive time is inversely proportional to the distance to sink node and is proportional to remaining energy. The node with more remaining energy and short distance to sink node has more chance to be the unique forwarding node.

The competition procedure for receiving node to be forwarding node is described as follows. Each receiving node can compute its forwarding competitive time. Before the competitive time, receiving node first detects busy signal. If busy signal is not detected, receiving node will send a request frame. The sending node receives request frame and sends a busy signal to stop other receiving nodes sending request frames. In this case, only a receiving node can be the node to forward data, and other nodes will drop received data.

Implementation of DDST scheme

The DDST protocol includes two critical code segments: receiving node–based protocol and forwarding competitive mechanism–based protocol. The main flow of protocol design is shown in Figure 6. Nodes in network are initialized. When the communication period comes and communication channel is idle, the first thing is to judge the role of node. If the node is a
sending node, it will broadcast its information to candidates and change its role. Candidates receive this information and compute the forwarding competitive time to select a unique forwarding node. After that, the information will be further forwarded to sink node.

The proposed algorithm is described as follows. All nodes are synchronized before starting the algorithm. First, sensor node senses data from neighboring nodes. On basis of received data and its own information, the node can judge whether it can be the receiving node. If both conditions are satisfied, the node will enter the competition of forwarding node. Otherwise, the node goes to sleep.

After that, random selection algorithm for forwarding node is performed. Based on the conditions of being receiving node, the forwarding node is randomly selected from receiving nodes. With the forwarding competitive time, forwarding node is selected for data forwarding. To address random data transmission, a distributed data transmission scheme is designed in WSN. This scheme uses multiple-path competition optimization between sending node and receiving node. Encoded data is transformed redundantly. After receiving enough redundant data, receiving node could decode it to get original data. When decoding fails, extra data transmission is necessary. This scheme could save communication overhead and have good security.

### Experimental analysis and comparison

#### Simulation parameters

In this section, simulation experiment is conducted to verify performance of DDST. Additionally, we analyze node number within sensing area and the effect of various constraint values on data transmission. The experiment platform is implemented by C++ language. Network simulator (NS2) is used to quantify performance in real environment. The nodes are randomly distributed in the target area. Here, the following parameters are considered: network size is set as $300 \times 300$ m$^2$. The number of nodes in experiment network is 200. On basis of network model, sensor nodes slowly move at a constant speed. In simulation, we set the speed of nodes to be 0.6 m/s. Sink node is fixed at position (120,120). Initial energy of each sensor node is 100 J. The communication radius ranges from 20 to 80 m. One time of data sending and data receiving consumes energy $2 \times 10^{-3}$ and $1 \times 10^{-4}$ J, respectively. The size of data package is 128 bytes. Each node can store 2048 bytes of data. All the parameters are set as shown in Table 1.

#### Comparison of network lifetime

Network lifetime is a critical indicator to evaluate performance of data transmission protocol in MSN. It can be described by the relationship between surviving nodes and running rounds of network.

Figure 7 compares network lifetime for three data transmission schemes, namely, RCF, FAD, and DDST. We simulate and analyze energy consumption of three schemes to evaluate network lifetime. In Figure 7, the number of nodes is set as 100. We conducted 850 rounds of experiments. The results show that DDST obviously improves surviving time of nodes by comparing to RCF and FAD. Although the time of first dead node in DDST is earlier than that of RCF, the node dies with a slow speed rate. Finally, the lifetime of DDST is longer than that of FAD and RCF. Because DDST uses data transmission based on receiving node, it is unnecessary to create global routing. Candidates are selected from neighboring nodes of sending node to receive data. In addition, a competitive mechanism based on forwarding time is proposed to select a unique forwarding node. The forwarding node transmits data instead of multiple nodes. It reduces energy consumption. So, DDST is an energy-efficient protocol. In design of this protocol, it weeds out the candidate receiving nodes continuously, changing it from working

| Table 1. Simulation parameters. |
|-------------------------------|
| Parameters | Values |
| Network size (m$^2$) | $300 \times 300$ |
| Number of nodes | 200 |
| Movement speed of nodes (m/s) | 0.6 |
| Position of sink node | (120,120) |
| Initial energy of nodes (J) | 100 |
| Communication radius (m) | 20–80 |
| Energy consumption in sending (J) | $2 \times 10^{-3}$ |
| Energy consumption in receiving (J) | $1 \times 10^{-4}$ |
| Packet size (bytes) | 128 |
| Storage space (bytes) | 2048 |

![Figure 7. Analysis of the nodes life cycle.](image)
state to dormant state to save energy. In addition, the forwarding time-based competitive mechanism makes the forwarding node be that of more energy. In this case, network lifetime is prolonged.

From Figure 8, all data transmission algorithms (RCF, FAD, and DDST) have the same rate to generate message. Some algorithms consume energy rapidly, so less data is transmitted. By comparing to above simulation results, DDST can obviously prolong network lifetime and have better performance of data transmission under energy constrained environment.

Under the same WSN environment, different transmission methods lead to different network lifetimes. As shown in Figure 8, under energy-constrained environment, DDST has long network lifetime and better security compared to other transmission methods because DDST is a dynamic distributed data transmission with less energy consumption. Compared to other methods, it consumes less energy and time in data transmission and prolongs network lifetime.

**Comparison of data transmission performance**

The authors compare the DDST scheme with several classic routing algorithms (RCF and FAD) in terms of routing performance and energy efficiency. We mainly consider three indicators including transmission success ratio, delivery cost, and delivery delay. Transmission success ratio is the ratio of the number of successful transmitted messages from source node to target node to the number of totally generated messages. Delivery cost is the energy consumption during data transmission. Delivery delay is the time interval of the message generated from source node and sent to target node.

First, we simulate RCF, FAD, and DDST with different communication radii and compare data transmission success rates. The experiment results are shown in Figure 9. Communication radius ranges from 10 to 60 m. Obviously, when communication radius ranges from 10 to 30 m, the hops from a node to sink node are increasing in three algorithms. DDST has set two conditions in selection of candidates. Candidates should satisfy both conditions, which makes the hops of DDST to sink node be less than that of other two methods. With the increase in communication radius, the superiority of DDST is not obvious.

We also compare the transmission performance with various number of sensor nodes. The simulation and comparison are illustrated as follows. Figure 10 shows transmission success ratio with different number of sensor nodes. With the increase in sensor nodes, DDST has superiority on data transmission success ratio.
compared with other schemes because DDST utilizes analysis of relative movement distance between nodes and transfer time competitive mechanism.

The performance on delivery cost and delivery delay is shown in Figures 11 and 12, which are better than other schemes. As shown in Figure 11, we assume the energy is unlimited. Under the same condition, the proposed DDST protocol has the minimum cost compared to other algorithms. RCF and FAD have high energy consumption and delivery delay. The use of secure model of node competition reduces frequency of using sensor nodes. So, the delivery cost and delivery delay of DDST are the minimum. The comparison of three indicators proves the transmission performance of DDST is encouraging.

Network security analysis

Attackers aim to acquire unauthorized accessed data, who are probably external intruders or network users. Due to the lack of security in data transmission, nodes in WSN are vulnerable to various illegal attacks by deploying or capturing nodes. We assume illegally deployed sensor nodes pretend to be normal network nodes. These nodes could steal confidential data or perform false data injection attack. Besides, it is able for attackers to capture many nodes in network. These nodes can be utilized for sending plenty of false data to consume network resource rapidly, such as energy, bandwidth, computation ability, and storage. If the transmitted data is attacked, we need to perform security analysis on attacks like forging, signature tampering, and collusion.

(1) Resistance against forging attacks. First, data transmitter sends a package including his false name. Other nodes cannot forge this false name; otherwise, it cannot pass the co-verification. The difficulty to forge the identity is equal to SHA-1 hash function.

(2) Resistance against signature tampering attacks. The key for encryption is generated using regeneration code. The privilege of decryption is controlled. Even the data transmitter is unable to tamper data. Besides, attackers cannot get information about the key. So, the data will not be forged and tampered. The key is generated in authentication of multiple network nodes. Single-node authentication cannot tamper the signature.

This article presents a distributed data transmission approach to address above issues. Each transmission of data package will generate a new path. Attackers can capture various data packages only by capturing or eavesdropping all possible routing paths. The multiple paths are generated by all participated nodes. By capturing a part of nodes will not change the result. So, it satisfies both the high efficiency and controllability.

We conduct data capturing experiments on three schemes (RCF, FAD, and DDST) to verify the relationship between probability of capturing data and network size $N$ in WSN. Figure 13 shows the experimental result. Network size changes from 2 to 12. When other conditions are the same, various values of $N$ have directive impact on RCF and FAD. The effect on DDST is lower. We have analyzed the reason. The larger $N$ is, the more the created disjoint paths of DDST are. So, the security is higher. Although larger value of $N$ can improve performance of RCF and FAD, DDST has
better security because its path selection is controlled by original node and intermediate node.

Conclusion

This article targets at security in data transmission and proposes a DDST approach. DDST divides data transmission into two stages, namely, constructing a collection of receiving nodes and selecting a unique forwarding node from this collection. DDST uses relative movement analysis and competitive mechanism based on forwarding time. This protocol achieves effective, rapid, and precious data transmission.

The main work is concluded as follows: (1) select proper nodes as data receivers among all neighboring nodes of the sender. The following two conditions are satisfied: candidate node will not move out the communication range in data transmission period and candidate node should be set within the intersection of communication area and the 60-degree-sector-oriented sink node. The candidates should satisfy both conditions. (2) The competitive mechanism based on forwarding time is used. After receiving data, the mechanism will compute forwarding competitive time itself with remaining energy $E_r$ and distance to sink node. The candidate with the minimum competitive time will be selected to forward data. Other nodes will drop the received data.

At present, data transmission in network mainly focuses on a single node. Data transmission among all nodes has various energy, computation ability, storage, sensing areas, and communication distances. So, we should simplify this issue to master the essence. The parameters of nodes in WSN are not always consistent due to various factors. In this case, reasonable allocation and scheduling on work period of nodes should be considered in secure data transmission. It reduces network energy consumption and prolongs network lifetime. The nodes in WSN have complex features, causing great difficulty in research. Compared to other wireless networks, the study is still in its infancy. So, research on secure data transmission in WSN will be a big challenge in future works.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the National Science Foundation of China (grant no. 61572188), Hunan Provincial Natural Science Foundation of China (grant no. 2016jj2058), Scientific Research Project of Hunan University of Science and Technology (grant no. E51697), and Scientific Research Fund of Hunan Provincial Education Department (grant no. 14A047).

References

1. Cui L, Ju HL, Miao Y, et al. Research on wireless sensor network. J Comput Res Dev 2005; 42: 163–174.
2. Xie K, Wang X, Wen JG, et al. Cooperative routing with relay assignment in multi-radio multihop wireless networks. IEEE/ACM T Networking 2016; 24: 859–872.
3. Mongiovi M, Singh AK, Yan X, et al. Efficient multicasting for delay tolerant networks using graph indexing. In: Proceedings of the 2012 international conference on computer communications, 2012, pp.22–30. Santa Barbara, CA: ACM Press, http://www-bcf.usc.edu/~kpsou-nis/Papers/indexing.pdf
4. Zhang S, Cao J, Chen L, et al. Locating nodes in mobile sensor networks more accurately and faster. In: Proceedings of the 5th annual IEEE communications society conference on sensor mesh and ad hoc communications and networks, San Francisco, CA, 16–20 June 2008, pp.37–45. New York: IEEE.
5. Zhang S, Cao J, Chen L, et al. Accurate and energy-efficient range-free localization for mobile sensor networks. IEEE T Mobile Comput 2010; 9: 897–910.
6. Xing G and Wang T. Rendezvous planning in wireless sensor networks with mobile elements. IEEE T Mobile Comput 2008; 7: 1430–1443.
7. Li G, Shi W and Wang Y. Automatic ARIMA time series modeling for data aggregation in wireless sensor networks. Int J Digital Content Tech Appl 2012; 6: 438–447.
8. Feng Y, Gong H, Fan M, et al. A distance-aware replica adaptive data gathering protocol for delay tolerant mobile sensor networks. Sensors 2011; 11: 4104–4117.
9. Lan F and Su W. A survey on sensor networks. *IEEE Commun Mag* 2002; 40: 102–114.

10. Zhang S, Zeng Y, Chen L., et al. Performance evaluation of localization algorithms for mobile sensor networks. *J Software* 2011; 22: 1597–1611.

11. Guo LJ, Raheem A and Li YS. SMITE: a stochastic compressive data collection protocol for mobile wireless sensor networks. In: *Proceedings of the IEEE INFOCOM*, Shanghai, China, 10–15 April 2011, pp.1611–1619. New York: IEEE.

12. Haneef M and Deng Z. Design challenges and comparative analysis of cluster based routing protocols used in wireless sensor networks for improving network life time. *Adv Inform Serv Sci* 2012; 4: 450–459.

13. Zhang J and Li L. Maximum life-time broadcast authentication protocol for wireless sensor networks. *Adv Inform Serv Sci* 2012; 4: 146–154.

14. Katti S, Rahul H and Hu W. XORs in the air: practical wireless network coding. *IEEE T Netw* 2008; 16: 497–510.

15. Wark T, Corke P, Sikka P, et al. Transforming agriculture through pervasive wireless sensor networks. *IEEE Pervas Comput* 2007; 6: 50–57.

16. Li Z, Li M, Wang J, et al. Ubiquitous data collection for mobile users in wireless sensor networks. In: *Proceedings of the IEEE INFOCOM*, Shanghai, China, 10–15 April 2011, pp.2246–2254. New York: IEEE.

17. Wang Y, Wu H, Dang H, et al. Analytic, simulation, and empirical evaluation of delay/fault-tolerant mobile sensor networks. *IEEE T Wirel Commun* 2007; 6: 3287–3296.

18. Maurice J, Chadi M and Fawaz F. Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges. *IEEE Commun Surv Tut* 2012; 14: 2–15.

19. Sha L and Gup T. An adaptive and efficient data delivery scheme for DFT-MSNS (delay and disruption tolerant mobile sensor networks). In: *Proceedings of the IEEE international conference on advances in engineering, science and management*, Nagapattinam, India, 30–31 March 2012, pp.99–104. New York: IEEE.

20. Zhang K, Zeng J and Liu W. Data delivery scheme of DTMSN based on probability replication and its performance research. *J Electron Inform Tech* 2010; 32: 677–681.

21. Carlo C, Rosario F and Marco L. DTN bundle layer over TCP: retransmission algorithms in the presence of channel disruptions. *J Commun* 2010; 5: 106–116.

22. Heinzelma WR, Chandrakasan A and Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: *Proceedings of the 33rd Hawaii international conference on system sciences*, Maui, HI, 7 January 2000, p.223. New York: IEEE.

23. Mohanty P and Kabat MR. Energy efficient reliable multi-path data transmission in WSN for healthcare application. *Int J Wireless Inform Network* 2016; 23: 162–172.

24. Srouji MS, Bonny T and Henkel J. High-speed encoding/decoding technique for reliable data transmission in wireless sensor networks. In: *Proceedings of the 2014 11th annual IEEE international conference on sensing, communication, and networking*, Singapore, 30 June–3 July 2014, pp.1449–1454. New York: IEEE.

25. Marappan P and Rodrigues P. An energy efficient routing protocol for correlated data using CL-LEACH in WSN. *Wirel Netw* 2016; 22: 1415–1423.

26. Rani S, Malhotra J and Talwar R. Energy efficient chain based cooperative routing protocol for WSN. *Appl Soft Comput* 2015; 35: 386–397.

27. Kim DS and Chung YJ. Self-organization routing protocol supporting mobile node for wireless sensor network. In: *Proceedings of the first international multi-symposiums on computer and computational sciences*, Hangzhou, China, 20–24 June 2006, pp.622–626. New York: IEEE.

28. Wang Y and Wu H. DFT-MSN: the delay/fault tolerant mobile sensor network for pervasive information gathering. *IEEE T Mobile Comput* 2007; 6: 1021–1034.

29. Li L, Jiang W, Sun L, et al. A receiver-based cross-layer forwarding protocol for mobile sensor networks. *Chin J Comput Res Dev* 2009; 46: 120–128.

30. Lu W and Li G. A prediction-based and low redundancy data forward strategy in mobile wireless sensor networks. *J Comput Res Dev* 2011; 48: 125–130.

31. Wang Y and Wu H. Replication-based efficient data delivery scheme (RED) for delay/fault tolerant mobile sensor network (DFT-MSN). In: *Proceedings of the 4th annual IEEE international conference on pervasive computing and communications workshops*, Pisa, 13–17 March 2006, pp.485–489. New York: IEEE.

32. Blum B, He T, Son S, et al. *A robust state-free communication protocol for sensor networks*. Charlottesville, VA: University of Virginia, 2003.