A Low Power Consumption Cryptography Algorithm Research for Wireless Sensor Networks

Lei Peng, Ying Xiao
Faculty of Electronics and Information Engineering,
Jinggangshan University,
Jiangxi Province, China
Key Laboratory of Watershed Ecology and Geographical Environment Monitoring,
National Administration of Surveying, Mapping and Geo-information Bureau,
Jiangxi Province, China
E-mail: penglei@jgsu.edu.cn, mengya11@126.com

***Abstract*-For the LEACH protocol during the process of cluster formation, only consider node its own communication cost disadvantage and security issues, through the analysis of the optimization design issues of single nodes and the network whole level of WSNs, a kind of security technology put forward to the clustering phrases proposed in this paper, and comprehensive consideration of the multi-hop improvement algorithm on node location and energy state. The simulation shows that the new algorithm save and balance energy consumption of each nodes, prolong the life cycle of the network and identify the malicious nodes based on key pre-distribution scheme and node ID information, in addition, prevent attack behavior from the beginning, which contribute to guarantee the authenticity and reliability of the message collection fundamentally, as well as enhance the survivability and robustness of the network to maximum.**

Keywords- wireless sensor networks; leach; clustering; low power consumption; algorithm

I. INTRODUCTION

Wireless Sensor Networks, namely WSNs, are composed of some preset sensors within a certain monitoring area, form an interconnected and orderly network system through the method of wireless communication. The development of WSNs was initially formed due to the military needs, and now, it has been widely applied in environmental and ecological monitoring and protection, traffic control and other civil areas. As new information acquisition and processing technology, has become a notable high tech fields in recent years.

Literature [1] shows that the WSNs research originated from the U.S. military in the foreign countries, which has been more than 20 years of history. The sensor networks have distinctive interdisciplinary research characteristics, which involve sensor technology, network communication technology, wireless transmission technology, embedded computing technology, distributed information processing technology, microelectronics manufacturing technology and software programming technology and multidiscipline. In the United States, almost all well-known colleges and universities have research team engaged in research on related techniques of WSNs; colleges and universities and research institutions in Britain, Germany, France, Finland, Canada, Japan, South Korea, Singapore, and other countries also have joined the ranks of WSNs research; many countries around the world input a large amount of human and material resources investment in large-scale research, and many related research results have been put into the application, but also many issues exist [2,3,4].

The research of WSNs started relatively late in China, generally considered to be from the beginning of the 21st Century to track the world trend of WSNs. At present, this country have the Institute of Shanghai Micro System, Computing, Software, Electronics and Shenyang Automation, Shenzhen Advanced Technology Research Institute and Hefei Intelligent Technology Research Institute, and other scientific research institutions within the System of Chinese Academy of Science. This paper, a low-power cryptographic algorithm for WSNs is proposed, which aims at reducing the energy consumption of wireless communication module.

II. ENERGY CONSUMPTION OPTIMIZATION ANALYSIS OF WSNS

Due to energy consumption of wireless communication module in WSNs takes up the most part in the whole network energy consumption, hence, it shows a particularly significant to the energy consumption optimization and design on wireless communication module, of which the method mainly contain two parts for WSNs: one is on single node layer, and the other is on whole layer.

III. SINGLE NODE LAYER OPTIMIZATION DESIGN OF WSNS

A low power consumption design of the single node mainly includes modulation mode option, short range multi-hop communication paradigm utilization, node sleep time addition and processor module low power design, etc.

To reduce the manufacturing cost of WSNs node, a low modulation method adopted to decrease the power consumption of node.

For WSNs, communication energy consumption E=kd，where d is a communication distance, k value is 2<k<4. It can be seen that communication energy consumption rise up dramatically with the distance decrease. Therefore, we take the measure to meet the communication rate conditions, and use the approach to shorten the communication distance for communication achievement.

It is assumed that the spatial distribution characteristic of an independent probability distribution event is $A_{xy}(x,y)$, A_{ck} indicates the probability that node k is obtained, and the average time rate of sensor areas R is α_{ck}. Then, there:

$$A_{xy} = \frac{\int_{ck} A_{xy}(xy)dxdy}{\int_{R} A_{xy}(xy)dxdy} \tag{1}$$

$A_K(t,n)$ indicates the probability of node event occurrence at t time, then:

$$A_k(T_{CK},0) = \sum_{i=0}^{\infty} \frac{e^{-\alpha_{ck}}(\alpha_{ck}T_{tn})^i}{i!}(1-A_{ck})^i \tag{2}$$

The probability of at least one event occurrence is:

$$A_{ck,n}(T_{ck}) = 1 - A_K(T_{CK},0) \tag{3}$$

It is assumed that the time of state transition occurrence is T1 and T2 respectively, then the energy saving calculation formula as follows:

$$E_{kd} = A_x * T_i - \frac{A_m + A_n}{2} * (T_{ck}, T_{dk}) - A_n * (T_i - T_{dk}) \tag{4}$$

The threshold value can be calculated out according to the above of formulas:

$$T_{i,th} = \frac{1}{2}[T_{dk} + (\frac{A_m + A_n}{A_m - A_n})T_{ck}] \tag{5}$$

It can be seen that, only T_i is greater than $T_{i,th}$, then energy saving can be achieved.

$$E_{kd} = E_{elec}(k) + E_{DMP}(k,d) = \begin{cases} kE_{elec} + kE - Ss^{d^2} \\ kE_{elec} + kE - mp^{d^4} \end{cases} \tag{6}$$

IV. A LOW POWER CONSUMPTION CRYPTOGRAPHY ALGORITHM OF WSNS

Through above analysis of power control issue on WSNs, a new power control algorithm based on node location is proposed, the algorithm complexity is not high and easy to run on the node.

A. *LEACH Protocol*

The LEACH is a low power self-adaptive hierarchical routing protocol designed for WSNs. This protocol, the nodes are self-organized into different clusters. Each cluster has only one cluster head, and all non-cluster head nodes send their data to the head node. In order to decrease the energy consumption of network, the cluster head node sends the data to the base station after data fusion.

V. LEACH PROTOCOL CLUSTER HEAD DATA SECURITY

The cluster head data security issue of LEACH is mainly present on three phrases, which are cluster establishment of each round, cluster establishment of LEACH and the accomplishment of cluster organization.

Firstly, for the cluster establishment stage of each round, the core issue is the process of cluster establishment phase, which is the key distribution model based on symmetric cryptography system, to achieve feasible key distribution scheme on low cost and power consumption with limited resources sensor nodes. Secondly, for the cluster establishment stage of LEACH, which nodes determined to act as cluster heads with the rated power, and broadcast the message of cluster heads are themselves to the network; otherwise, the non-cluster head nodes only simply choose the original nodes with the strongest signal can be received as the cluster heads joined by themselves. Finally, it enhance the capacity of node damage due to the power constraints of sensor node itself, in addition, reduce or lower a large number of isolated nodes caused by attacker after cluster organization in WSNs.

VI. LOW POWER ENCRYPTION ALGORITHM OF WSNS

To eliminate security risks for LEACH, it is necessary to have the following functions: 1) Selecting the cluster to be added by non-cluster node, the legitimate identification and link double-way authentication for the declared cluster head node before sending formal joint request. Link bidirectional authentication is to ensure a hop up communication link existence between non-cluster head nodes within their power scope and so-claimed cluster head node, in addition, node only send adding cluster message to the legitimate one with the strongest signal. 2) To prevent attackers from retransmitting by simply amplifying the power of the stealing heard news, it requires LEACH protocol also has the ability to resist the replay attack.

VII. ASSUMPTION AND BASE STATION INITIALIZATION

Assumption: each node shares a pair of main key Kmaster with credible base station; and shares one-way key generating function f (x), Ki=F(Ki+1); ordinary nodes with enough power to transmit data packets to the base station when needed.

Initialization: the base generates a key pool and determines the key synchronization clock. The size of the key pool N depends on the storage space of the base, the network lifetime and broadcast frequency, etc.

$$IK_u = f_{K_m}(u) \tag{7}$$

Above formula (7), f indicates the pseudo random number, u indicates the node u identity symbol, k_m represents the main key stored in the base station, and IK_u represents the individual key of node U.

VIII. CLUSTER HEAD KEY ESTABLISHMENT PROCESS

It is assumed to be able to establish the minimum time for the key during the process of the cluster head key establishment to be T min, and the specific establishment process of cluster head key consists of the following four steps.

Step 1: Cluster Head Key Pre-configuration Phase.

The initial key KIN generated randomly by the base station, at same time, the key KIN loaded into each sensor node through pre-configuration method. An arbitrary node of sensors as u, determines to be a cluster head or not through formula (8) on the basis of utilizing key KIN and its own ID derived from a main key and LEACH protocol algorithm.

$$K_u = f_{K_{im}}(u) \tag{8}$$

Step 2: Neighbor Discovery Phase.

After nodes deployment, an arbitrary node u first initialize a key synchronization interval value Tmin, calculate n=Tround/Tmin（Tround is the time needed for protocol run a round), the time Tmin is the minimum time neighbors found. After the initialization complete, the node u starts the neighbor discovery process. Firstly, node u send a broadcast message to the surrounding, then reply response message when neighbor node V received a broadcasting message from the node u, the message as follows (9) and (10) respectively.

$$u \rightarrow * : u \tag{9}$$

$$v \rightarrow u : v, MAC(K_V, u|v) \tag{10}$$

Step 3: Establishment Stage for Key.

Node u receives response message from neighbor node v sends, calculated out the main key Kv of node v by the formula (8), number the cluster head in accordance with the cluster head packet arrival sequence, determine key chain for the cluster heads new arrival, while the node v certification completion. If authentication is passed, then pair key Kuv calculation between them by formula (11) the. Node v uses the same method to calculate the pair of keys.

$$K_{uv} = f_{K_v}(u) \tag{11}$$

Step 4: Key Delete Phase.

After the ending time of Tmin found by the neighbor, the node u wound remove the key KIN and its neighbor node V's main key Kv. Note: node u does not delete their own main key Ku, as well as other nodes wound not delete their own master key.

IX. SIMULATION AND ANALYSIS

A. Simulation

NS simulator [12] as experimental platform adopt in this paper to simulate and analyze the WSNs low power consumption encryption algorithm based on LEACH protocol, and carry out the performance comparison. The simulation scenario area size is 100m×100m, and randomly distributes 50 sensor nodes with the same type and a base node. The parameters as shown in Table 1.

TABLE I. SIMULATION PARAMETERS

Parameters	Unit	Data	Parameters	Unit	Data
Common node transmission power	W	0.036	Common node Receiving power	W	0.024
Initial energy	J	10	Transmission range	M	100
Base station node transmision	W	0.5	Base station node receiving power	W	0.5
Initial Energy	J	100	Transmission range	M	100
The number of cluster heads	Z	20%	Rounds of running time	C	5

X. ENERGY CONSUMPTION ANALYSIS

It can be shown that the implementation of security strategy has a limit influence on common node energy consumption by comparison with figure 1. Each node residual energy presents a linear relationship after running the 15th rounds by protocol. This mainly due to the same attention given to energy and security consciously at the beginning. And through the base station and cluster head node as far as possible to undertake the additional energy consumption from security policy, and achieve the goal of balance and ordinary sensor nodes energy consumption decrease.

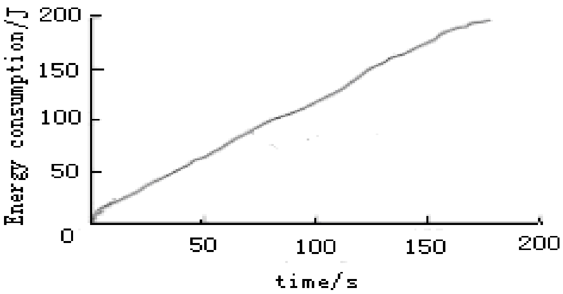

Figure 1 Enery Consupmtion Analysis Diagram

XI. CONCLUSION

The low power consumption cryptography algorithm is particularly suitable for the industries of garden irrigation to plants dying prevention in the condition of low humidity; red alert to breaching of the dike prevention in the condition of river water level being over top; promptly traffic light time transformation to traffic diversion in the condition of congestion, such as flood monitoring and early warning in middle–lower reaches of the Gan River, ecological environment survey and control protection in Poyang Lake, urban traffic intelligent control system and other fields, to realize high efficiency and intelligence scientific management.

ACKNOWLEDGEMENT

The Natural Science Foundation of Jiangxi Province (No., 20122BAB211039), Low Energy Consumption Clustering Algorithm on Wireless Sensor Network.

REFERENCES

[1] Liu, Zhixin, et al. "A distributed energy-efficient clustering algorithm with improved coverage in wireless sensor networks." Future Generation Computer Systems 28.5(2012):780-790.

[2] Wang, Aimin, D. Yang, and D. Sun. "A clustering algorithm based on energy information and cluster heads expectation for wireless sensor networks." Computers & Electrical Engineering 38.3(2012):662-671.

[3] Chang, Jau Yang, and P. H. Ju. "An efficient cluster-based power saving scheme for wireless sensor networks." Eurasip Journal on Wireless Communications & Networking 2012.8(2012):648-650.

[4] Chang-Ri, Luo, et al. "A Clustering Algorithm Based on Cell Combination for Wireless Sensor Networks." Education Technology and Computer Science (ETCS), 2010 Second International Workshop on IEEE, 2010:74-77.

[5] Chugui, X. U., X. Deng, and H. Zou. "Repair Policies of Coverage Holes in Wireless Sensor Networks." Chinese Journal of Sensors & Actuators23.2(2010):256-259.

[6] Zhang, Pengfei, G. Xiao, and H. P. Tan. "Clustering algorithms for maximizing the lifetime of wireless sensor networks with energy-harvesting sensors." Computer Networks 57.14(2013):2689-2704.

[7] Yang, Fan, K. C. Wang, and Y. Huang. "Energy-Neutral Communication Protocol for Very Low Power Microbial Fuel Cell Based Wireless Sensor Network." IEEE Sensors Journal 15.4(2015):2306-2315.

[8] Sun, Qingquan, et al. "Primate-inspired adaptive routing in intermittently connected mobile communication systems." Wireless Networks20.7(2014):1939-1954.

[9] Huang, Xin Lin, et al. "QoS-Adaptive Routing Protocol Design for Multi-Hop Cognitive Radio Networks Considering Multi-Link Interference."International Journal of Sensors Wireless Communications & Control1.2(2012):88-92.

[10] Jain, Yogendra Kumar, et al. "Min Max Normalization Based Data Perturbation Method for Privacy Protection." (2011).

[11] Kang, Sang H., and T. Nguyen. "Distance Based Thresholds for Cluster Head Selection in Wireless Sensor Networks." IEEE Communications Letters 16.9(2012):1396-1399.

[12] Jain, Tapan. "Tapan Jain, “Wireless Environmental Monitoring System (WEMS) Using Data Aggregation in a Bidirectional Hybrid Protocol,” ICISTM 2012, France, pp 414-420. 2012, 10.1007/978-3-642-29166-1_38. " Icistm.

[13] Patra, C., et al. "A reliable two-tier energy-efficient topology building algorithm for Wireless Sensor Networks." Applications and Innovations in Mobile Computing IEEE, 2014:146-150.

[14] Sabet, Maryam, and H. R. Naji. "A decentralized energy efficient hierarchical cluster-based routing algorithm for wireless sensor networks."AEU - International Journal of Electronics and Communications69.5(2015):790-799.