Sensors & Transducers, Vol. 170, Issue 5, May 2014, pp. 137-142

www.sensorsportal.com

Sensors & Transducers

http://www.sensorsportal.com

Algorithm for Wireless Sensor Networks Based on Grid Management

[1] Geng Zhang, [2] Hao Xu

[1] Chongqing Technology and Business Institute, No. 1, Hualong Avenue, Jiulong Science and Technology Park, Jiulongpo District, Chongqing City, 400052, China
[2] Chongqing Electric Power College, Wulong Temple, Jiulongpo District, Chongqing City, 400053, China
[1] Tel.: +8618523073848, fax: 118523073848
[1] E-mail: zzwqydb@126.com

Received: 3 March 2014 /Accepted: 30 April 2014 /Published: 31 May 2014

Abstract: This paper analyzes the key issues for wireless sensor network trust model and describes a method to build a wireless sensor network, such as the definition of trust for wireless sensor networks, computing and credibility of trust model application. And for the problem that nodes are vulnerable to attack, this paper proposed a grid-based trust algorithm by deep exploration trust model within the framework of credit management. Algorithm for node reliability screening and rotation schedule to cover parallel manner based on the implementation of the nodes within the area covered by trust. And analyze the results of the size of trust threshold has great influence on the safety and quality of coverage throughout the coverage area. The simulation tests the validity and correctness of the algorithm. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Trust management, Grid, Wireless sensor networks, Rotation scheduling, Retreat mechanism.

1. Introduction

With the development of communication technology and sensor technology, the micro-sensors with low power consumption, low cost, versatile, etc. began to play an important role in various fields. Wireless sensor networks (WSNs) is composed by a large number of micro-sensor wireless networks, its value lies in the real-time monitoring, sensing, collecting information and monitoring of various environmental objects distribution network within the region, and this information is processed to obtain detailed and accurate information, and transmit information to the user [1]. However, because less energy wireless sensor network nodes and a simple structure and other shortcomings, led to its failure or vulnerable to attack and can not continue to work, reducing the quality of services provided WSNs, shortening the life cycle of WSNs. This security technologies for WSNs put forward higher requirements.

Wireless sensor network nodes with limited resources, network nodes subordinate institution under normal circumstances, without the use of trust management authorization certificate ways. The trust management into every aspect of the wireless sensor design is only in recent years of new ideas put forward. At present, for trust management of wireless sensor networks focused on trust in nodes evaluated by assessing the degree of trust to enhance the security of wireless sensor networks, robustness and so on.

2. Research of Trust Mechanism About Wireless Sensor Network

2.1. Trust Demands of Wireless Sensor Network

With the application of wireless sensor network becomes more and more complex, also present diversity of its safety, need to introduce effective mechanism timely identification of captured nodes, targeted to take corresponding measures to reduce the loss of system. The trust mechanism in wireless sensor network, it is on the network attacks in wireless sensor networks to enhance immunity, enhance the security and availability of network security as the goal, is to avoid or deal with the illegal intrusion, malicious attack. But trust is to promote interaction or business cooperation in the network environment, the risk and substantive cooperation to reduce. Both are closely linked, security can provide reliable communication and information protection for the trust is created, trust can be used to enhance security [2].

2.2. Design Principle of Trust Management of Wireless Sensor Network

Trust management system of wireless sensor network provides an integrated management mechanism, to effectively monitor and control the remote environment or managed entity, in the network to solve the internal attack, identify the malicious nodes, selfish nodes and nodes with low competitiveness, and with less energy consumption of network resource allocation for unified management and maintenance. In order to achieve this objective, the trust management system design should follow the following principles [3]:

1) Lightweight structure.

In the network layer protocols in safe conditions, as simple as possible, they should try to avoid too much storage and processing requirements to increase the node resource requirements. A lightweight protocol to ensure that nodes in the network resources are not very fast consumption, prolong the network life cycle.

2) Intelligent mechanisms of self-organization

Wireless sensor network after deployment, rarely artificial intervention, the deployment of nodes in an ordered network from the disordered state through mutual communication, the ability of self-organization network is one of the key factors for successful completion of this configuration.

3) Simple, effective trust model

Trusted computing is the core of trust management system in the network through trust degree calculation model obtained, should be accurate. The real show current status of network nodes, at the same time, the calculation of trust degree, also should not need to consume large amounts of resources and complex operation.

4) Safety, stable internal environment.

The deployment of diversity and abominable environment of wireless sensor network, requirements management system structure of wireless sensor network must ensure that the management of information and data exchange between nodes are safe. Not only have the ability to resist external attack, also need to be able to identify malicious nodes in the network.

3. Model of Trust Management

3.1. Grid Point Trust Models

Mesh grid point is a virtual form of the target area, the intersection of the horizontal and vertical coordinates that when meshing. Trust with grid points of a circle, the radius to-node communication within a radius of active nodes (node trust than the trust threshold) parallel to the grid points covered, after quantization, finally get through the mesh points. This model is based on the following assumptions [4]:

1) Can get the wireless sensor nodes and mesh points and through some positioning algorithm, that marked these points.

2) Limit the size of the virtual grid at $\min(\sqrt{2}/4Rc, \sqrt{2}/2Rs)$.

For the following description of the model is more convenient, we define some symbols. T_{min}: Node trust threshold, the trust is below the threshold of a node is determined to be malicious nodes. (The threshold is determined by the selected trust management model, the number of nodes and other factors) T_{max}: grid points combined trust threshold, the trust if the quantization grid points below the threshold can not guarantee the quality and safety of the coverage area [5] (The threshold value is determined by the number of nodes and the surrounding work their confidence factors). Na: indicates the degree of confidence in the malicious node, the node is less than T_{min}. Nb: expressed as dormant nodes, the nodes trust although higher than T_{min}, but after the final round-robin scheduling algorithm is judged to be redundant nodes. Nc: expressed as a working node, the node is higher than trust T_{min}, and after rotation scheduling algorithm active nodes.

Select the node trust model grid points results indicated in Fig. 1 below.

Process selection work node specific, will be in the next node scheduling algorithm based on adaptive rotation about grid trust description. As shown in Fig. 1, using the grid point as the center, Rs radius range of active nodes and the quantization of the grid, the grid point combined with trust degree. If the trust of all grid points are higher than the confidence threshold T_{max}, indicating that the coverage area has reached a high coverage and security requirements [6]. If a grid point trust degree is lower than a threshold value T_{max}, that are not up

to the high coverage of security requirements, is the need for scheduling re amounted to less than the requirements of grid point.

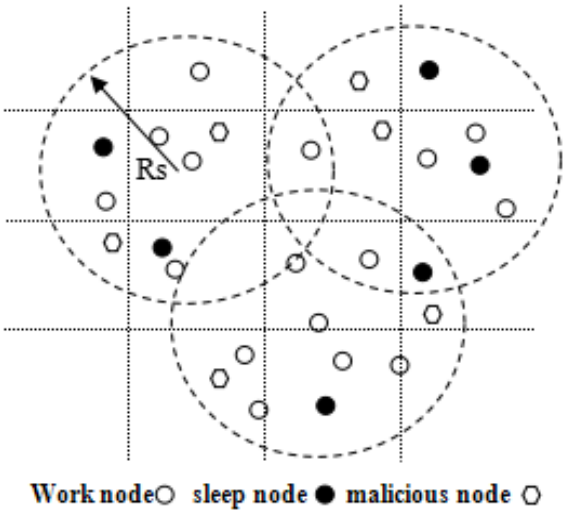

Fig. 1. Results of node selection by grid trust model.

3.2. Grid Point Trust Mathematical Model

In order to make the security of grid points within the sensing radius can have better, more than half of the required probability of working nodes sensing radius within the normal working than grid point confidence threshold T_{max}, so as to ensure the normal operation of the network.

The sensing radius assuming the grid points of W_{ij} within the n a more trusted nodes (over node trust threshold T_{min} node), trust degree difference for T1, T2, T3, ..., Tn, namely trust set S={T1, T2, T3, ..., Tn}. 'S' represents a collection of all aware error node trust composition, where 'm' denotes the number of nodes sensing errors, 'k' says one possibility [7]. For example, S21={T1, T2} represents the perceptual error node has two, {T1, T2} is one possible error node. The grid trust model is:

$$T_{Wij}=\sum_{m=1}^{\frac{n-1}{2}}\left\{\sum_{k=1}^{C_n^k}\left[\Pi_{T_\alpha\in S_{mk}}\left(1-T_\alpha\right)\Pi_{T_\varepsilon\in(s-s_{mk})}T_\varepsilon\right]\right\}+\prod_{\sigma=1}^{n}T_\delta \tag{1}$$

Among them, T_α said trust aware error node, T_ε said trust work node, $\Pi_{T_\varepsilon\in(S-S_{mk})}T_\varepsilon$ product for all appropriate perception trust degree of nodes, set $S\text{-}S_{mk}$ to normal working nodes of the mesh point perception within the radius of trust. Only trust all coverage of the target area of grid points are reached the threshold of T_{max}, to indicate that this is a safe cover.

4. Algorithm Description of Node Adaptive Rotation Scheduling Based on Grid Trust

In this section designed a grid covering algorithm based on trust to schedule sensor nodes, making the monitoring area to achieve high security coverage.

4.1. Summary of the Algorithm

Covering algorithm presented in this paper is a fully distributed algorithm, called the split pair coverage throughout the coverage area of the coverage of each grid point within the region, finally achieves the same or higher coverage effect. The covering algorithm is not only to solve the trust management and covering a combination of problems, but also consider the activity node trust change influence on the coverage area, and trust based backoff mechanism design problem.

In the network coverage in the process, every cycle, trust related working nodes may change. If the trust degree of nodes becomes small, will lead to a grid trust overlay can not reach the standard T_{max}. Need to directly increase the working nodes at the start of a new cycle, in order to ensure the reliability of the network. As shown in Fig. 2(a), as one of the trust degrees of nodes is reduced from 0.8 to 0.7, the new operating cycle (b), the scheduling algorithm, the grid points within the sensing area adds a new trust nodes of degree 0.9, to reach the required standard.

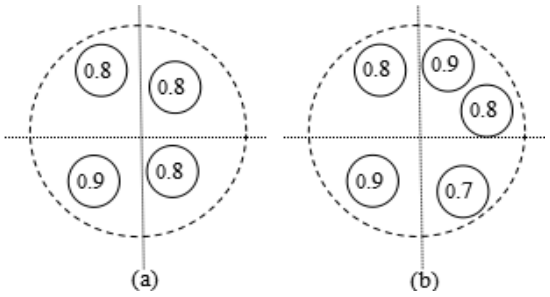

Fig. 2. Effect of node trust changes on the grid point sensing region.

4.2. Algorithm Design

The communication model and the perceptual model of wireless sensor nodes are disc model. Among them, the grid point W_{ij} as the center of a circle, radius circular region for the sensing radius Rs sensor node, called the sensing area of the grid points of R. Said sensor nodes in grid point sensing region is the related nodes, other nodes not related. That is:

$$\Omega_{ij} = \{n / d(n, W_{ij}) < Rs\}, n \in N \ , \quad (2)$$

Ω_{ij} denotes the set of grid points of related nodes, 'N' in order to cover all nodes within the region. D (n, W_{ij}) represents the node to the grid point distance, the distance is less than 'Rs', add to the set Ω_{ij} . The sensor nodes N1, N2, their coverages of the region are S1 and S2 respectively, if $S1 \bigcap S2 \neq \Phi$, the sensor node coverage. In the grid point sensing region 'R' and does not participate in the scheduling of dormant nodes, with 'X' denotes the set of these nodes. At the same time with 'G' said participating node coverage task set.

In order to better illustrate the algorithm implementation process, the concrete steps of the algorithm described as follows:

1) Virtual grid division of target area, and determine all the grid points within the target region position (x, y). Find grid point Ω_{ij} by all collection of related nodes.

2) Determine trust degree of all relevant grid point within the target area: if $T<T_{min}$, the node is determined as the malicious nodes, removed from the grid node, not participate in any scheduling; if $T>T_{min}$, then the node is determined as the active node, into the active node set, active node set is denoted as 'H'.

3) In order to ensure the coverage process node, use as little as possible and keep higher security, prolonging the life cycle. The set of nodes in 'H' according to the quantity from less to more, the trust degree of the order from high in the end into the node set 'G1'. For example, the first set 'H' trust in the highest node in 'G1', if the node's trust can reach T_{max} standard, the grid points to be working set is the node; otherwise, continue to set the highest node H in the set 'G1', determine the grid point joint trust degree is reached requirements. And so on, finally determined to work node all grid point set 'G1', while the remaining active nodes into sleep set to 'X1'.

4) In the selection phase of each node, the node will broadcast to all neighbor nodes information perception radius (including the node number, location and trust). When gathering information, if the judge is redundant coverage node, in order to avoid the emergence of coverage blind, introduced a backoff mechanism based on trust, for each work whether the node dormancy wait for a random period of time 't', after the time to determine whether to stay dormant.

For the relevant node N1, N2, if they trust degree for Tn1, Tn2, then set the timer as:

$$T_{tb}^{(n1)} = k\left|1 - T_{n1} / T_{\max}\right| \bullet t_{n1}, \quad (3)$$

$$T_{tb}^{(n2)} = k\left|1 - T_{n2} / T_{\max}\right| \bullet t_{n2}, \quad (4)$$

t_{n1} , t_{n2} is the current time, 'k' is regulation parameter of the system, and it can be set according to the actual situation.

The following backoff mechanism specific: if $T_{tb}^{(n1)} = T_{tb}^{(n2)}$, then work node selects the node number is; if $T_{tb}^{(n1)} \neq T_{tb}^{(n2)}$, then select nodes with high trust as working nodes.

All the dormant state to not enter dormancy nodes to be determined, but wait for the trust degree of grid point coverage is determined, according to the size of grid trust, finally decided to stay dormant nodes are dormant or re scheduling for becoming a working node. Will ultimately determine the dormant nodes into the dormant node set 'X', ultimately determine the working nodes in a node set 'G'.

5) All related working nodes quantify grid point in the sensing region, get the trust 'T_w'. Next node scheduling is divided into two kinds of situation; 1, if $T_w \geq T_{max}$, showed complete credible high coverage grid point sensing area requirements, to be dormant nodes become dormant node; 2, the trust degree of $T_w < T_{max}$, which indicates that the grid point sensing area coverage does not reach the trust of high coverage requirements, activate grid point sensing region the highest level of trust to be dormant node becoming a working node [8]. The working nodes into the grid trust quantification process, re calculating trust degree. If $T_w \geq T_{max}$, ultimately determine the sleeping nodes and node; otherwise, the process is repeated, until the grid trust meet the above requirements [9].

6) Selected nodes, node scheduling into second stages: the stage. Related to the implementation of the monitoring task, until the end of the period.

Life cycle of the network is to repeat the process, until the network completely unable to work.

5. Experimental Results and Analysis

In order to verify the validity of the proposed algorithm is effective and the analysis, using Matlab 7.5 as the simulation platform of experiment and the analysis of its. The simulation experiment environment for the monitoring region size 100 m×100 m, 40~200 nodes are randomly distributed in the target area, sensing radius 10 m and the radius of communication nodes for 30 m. The algorithm of trust value is a trust management model based on reputation (RFSN) which is put forward by Ganeriwal-Srivastava in literature [10].

The proposed scheduling algorithm based on overlay nodes trust model and the Node Self-Scheduling document based on literature [12] node adaptive rotation scheduling algorithm and literature [11] grid trust (NSS) of the covering algorithm for performance comparison. The simulation results are shown in Fig. 3- Fig. 5.

Fig. 3 shows three different algorithms with running time of network, the coverage rate.

With the increase in the proposed changes little coverage algorithm, reach the 280th round, coverage rate can reach more than 80 %, while the other two algorithms are less than 80 %. The literature [11] without using the rotation scheduling algorithm, the node does not have the very good scheduling, fast energy consumption. Node Self-Scheduling (NSS) covering algorithm easy to meet emergencies in the node in the work process, lead to the decline of the overall quality of coverage [13]. The covering algorithm based on trust management, to the point of a grid must reach the confidence threshold can be determined, so the nodes in the work process does not get out of the situation. Due to the adoption of the grid points is parallel coverage, even if the node status and other related nodes to ensure the quality of coverage.

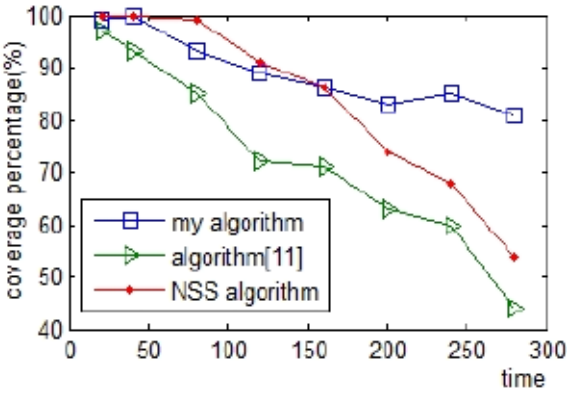

Fig. 3. Quality comparison of network coverage.

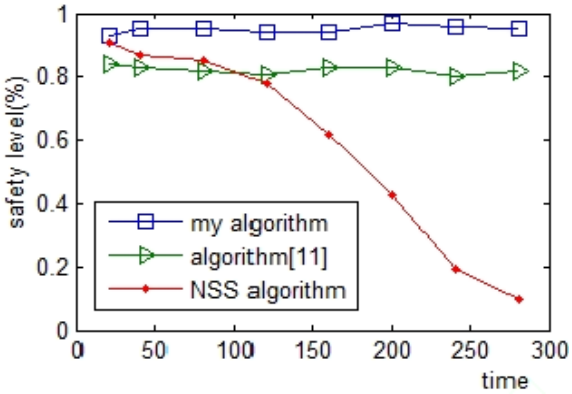

Fig. 4. The security level changes with time.

Fig. 4 reaction is three kinds of different algorithms with the increase of the network operation time, their coverage area safety degree of change. The definition of node safety behavior refers to does not have correct behavior of malicious attacks and camouflage problem node aging etc. [14]. As can be seen from the chart, with the increase in time of this algorithm and literature [10] algorithm of literature coverage degree of safety has not changed much, but this algorithm is a much higher degree of safety, this is due to the combined coverage mechanism for grid based on trust, improve the probability of node security behavior, which requires the coverage area must have a higher degree of safety.

Fig. 5 shows relationship between total energy and network remaining running time three different algorithms along with the network running time, the total residual energy. As can be seen, the lifetime of network by literature [9] is the shortest, this is because of all the nodes in a working state, the energy consumption of fast. The other two nodes are using the node rotation scheduling, to prevent the excessive consumption of energy. This algorithm considers the node may repeat coverage problem, thus the overall energy consumption more slowly, longer network lifetime.

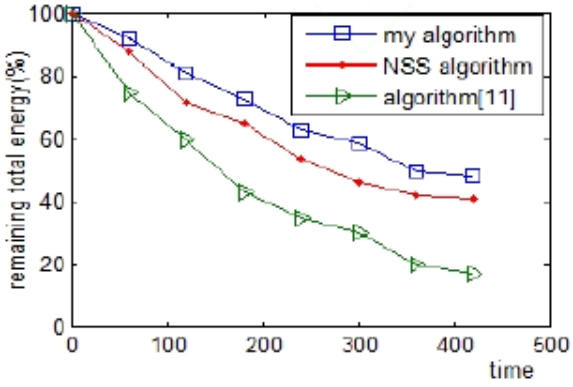

Fig. 5. Relationship between total energy and network remaining running time.

6. Conclusions

Aiming at the problem of trust management, this paper proposes a node adaptive rotation scheduling algorithm based on grid trust. Based on a deep understanding of the trust management framework, first proposed the grid trust model. Based on node credible, quantify grid point in grid point communication range, in order to achieve high coverage of regional trust requirements. At the same time, the algorithm uses a backoff mechanism based on trust, avoid blind spots and save energy, at the same time accurate selection of working nodes. Simulation results show that, the node adaptive rotation scheduling algorithm based on grid trust, not only can accurately ensure coverage quality requirements, but also can effectively reduce the error rate of network communication, the security of network environment, provide new ideas and theoretical basis for trust management framework of wireless sensor network.

Acknowledgements

Foundation Item: Research and Applications of Ad-hoc Network Type Fire Monitoring System.

Foundation Number: KJ131602.

References

[1]. Jianzhong Lee, Hong Gao, The research progress of wireless sensor network, *Journal of Integrative Plant Biology*, 45, 1, 2008, pp. 1-15.

[2]. Jianpin Wang, Ming Lee, Xianwei Zhou, Based on reputation and trust group of wireless sensor network entity authentication, *Chinese Journal of Structural Chemistry*, 21, 10, 2008, pp. 1780-1784.

[3]. Kai Feng, Study of trusted model in wireless sensor network based trust management, *Wuhan University of Technology*, 2009.

[4]. Ke Jing, Liyong Tang, Zong Chen, Trust management in wireless sensor networks, *Journal of Software*, 19, 7, 2008, pp. 1716-1730.

[5]. Blaze M., Feigenbaum J., Lacy J., Decentralized trust management, in *Proceedings of the IEEE Symposium on Security and Privacy*, Washington, DC, America, 16-19 March 1996, pp. 164-173.

[6]. Chao Wang, Xiangyu Jia, Qiang Ling, Based on the credibility of the wireless sensor network security routing algorithm, *Journal on Communications*, 29, 11, 2008, pp. 105-112.

[7]. Qiang Xu, Yun Wang, In the reliable fault-tolerant wireless WSN energy-efficient solutions of the problem, *Journal of Software*, 17, 11, 2006, pp. 184-191.

[8]. Han K. E., Application of Error Control Coding in Wireless Sensor Networks, *Sensors & Transducers*, Vol.158, Issue 11, November 2013, pp. 55-59.

[9]. Zhenya Yan, Baoyu Zheng, Trusted node selection algorithm in wireless sensor networks, *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition)*, 28, 2, 2008, pp. 11-13.

[10]. Shaikh R. A., Jameel H., D'auriol B. J., *et al.*, Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks, *IEEE Transactions on Parallel and Distributed Systems*, 20, 11, 2009, pp. 1698-1712.

[11]. Ganeriwal S., Srivastava M. B., Reputation-based framework for high integrity sensor networks, in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Network*, Washington DC, America, 16-19 March 2004, pp. 66-77.

[12]. Yin Zhen-Yu, Zhao Hai, Lin Kai, *et al.*, A coverage-preserving node scheduling scheme based on trust selection model in wireless sensor networks, in *Proceeding of the 1st International Symposium on Pervasive Computing and Applications*, Urumqi, China, 2006, pp. 696-698.

[13]. Tian D., Georganas N. D., Node scheduling scheme for energy conservation in large wireless sensor networks, *Wireless Communications and Mobile Computing*, 3, 2, 2003, pp. 271-290.

[14]. Hu Linna, Cao Ning, Sun Yu, Research on Distributed Video Compression Coding Algorithm for Wireless Sensor Networks, *Sensors & Transducers* Vol.154, Issue 7, July 2013, pp. 51-55.