International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.159-172
http://dx.doi.org/10.14257/ijsia.2016.10.8.14

Research on Intrusion Detection Technology Based on Nodes Optimization Deployment in Wireless Sensor Networks

Zeyu Sun[1,2], Longxing Li[1] and Xuelun Li[3]

[1]*School of Computer and Information Engineering, Luoyang Institute of Science Technology, Henan, Luoyang 471023, China;*
[2]*School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shanxi 710049 China*
[3]*School of Electronic information Engineering, Tianjing University, Tianjing 300072, China*
E-mail:lylgszy@163.com

Abstract

Security issues of wireless sensor networks (WSNs) have become increasingly prominent. As a reasonable complement for encryption, authentication and other security mechanisms, intrusion detection technology has become an important domain of WSNs security research. So it has very academic and practical value to design an intrusion detection approach adapting to wireless sensor networks characteristics. At the basis of the reputation computing model we designed, and after analyzing features of the sensor networks intrusion detection mechanism, we proposed an intrusion detection model based on trusty nodes inside clusters make use of the reputation computing model to calculate the coordinate nodes synthetic reputation values to check whether some invasion has taken place. If some nodes are being intruded, the messages will be reported to cluster head. When the numbers of the reporting nodes are more than the specified the head will report the information to sink nodes and start intrusion response at the same time. The experimental results show that the designed models can identify vicious nodes and low competitive nodes, helping to promote the security and reliability of the network, and embodying the equity of the network.

Keywords*: wireless sensor networks (WSNs); intrusion detection technology; trust management; behavior trust; reputation model*

1. Introduction

With the rapid development of information technology, wireless sensor networks have been in the field of military defense among various engineering, environmental monitoring, disaster relief, traffic engineering, intelligent home, health and other fields has been widely used [1-2]; wireless sensor networks organizational forms for the system: a random scatter deployed in the monitored area, through self-organizing multi-hop fashion between sensor nodes to complete a new network architecture for data collection, computing, communications, storage and other properties [3-5]. Since the deployment of the initial stage of randomness and uncertainty in the sensor nodes in the monitoring area somewhere will inevitably gather a large number of sensor nodes; and vice versa. Sensor networks, such as the existing authentication. Key management for security technology almost all belong to the passive method of prevention, lack of adaptability of intrusion, Intrusion Detection Technology Surgery is a proactive security technology defense in depth attacks; it monitors the host's operating status [6-8]. The method of state and network traffic to discover intrusion and abuse the privileges of the legitimate user behavior, as Against the invasion promptly provide important information to prevent the

ISSN: 1738-9976 IJSIA

occurrence of events and the expansion of the event, the network security the key component of the whole. Credible research network has become a hot topic trusted network technology is in the original there increase network security technology based on the behavior of credible security ideas, and strengthen the network status.

Dynamic process for the implementation of intelligent network security and quality of service that provide policy-based adaptive control foundation trusted network mainly includes three aspects: Trusted service provider network information transfer lose credibility and the credibility of end users thoughts and trusted network intrusion detection sensor with junction together, by checking the credibility of user behavior to identify malicious nodes. Selfish nodes for wireless transmission development and application of sensor network intrusion detection technology to provide a new method, has important theoretical research value and practical value.

2. Analysis of Security Technology

Micro processing power and wireless communication capabilities of wireless sensor network node of the wireless sensor networks have wide broad application prospects, such as the military, Environmental Monitoring, Medical, Intelligent buildings and other commercial areas [9-10]. However, in most applications environment for security of wireless sensor networks have a very high demand, therefore, security costs the key issue "for the further restrict unlimited sensor network is widely used, however, since the wireless sensor of the present body characteristics, wireless sensor network security is not an easy thing [11-12]. These characteristics of wireless sensor networks to the wireless sensor network security has brought new requirements, so most of the security mechanisms and security protocols are difficult to use the wireless sensor networks, wireless sensor design also makes network security has become a challenging job.

Because there are many restrictions in wireless sensor networks, such as the ability to limit node, you can only use symmetric key technologies and HASH; limit the ability of such unlimited power sensor networks should minimize communication, because the ability to communicate than the calculated power-consuming power "In addition, sensor networks also need to consider exchange poly reduce data redundancy and other issues, therefore, traditional methods can’t be applied to key management sensor network [13]. The current key management scheme based on a preconfigured divided into key programs and based on the group's key management KDC Management scheme. Key Management is pre-configured node prior to deployment, the key pre-configured in the node, provisioning key programs are usually set by the stored secret session key is calculated, because the node storage and energy limits system, pre-configured key management scheme must be considered to save storage space and reduce communication overhead, there are very multi preconfigured based key management scheme of such key management scheme is very simple, usually it requires computing load small strong network expansion capability to support dynamic changes of the network; but usually can’t support it, for authentication neighbor nodes; node after being captured, easy to disclose the entire network key. Group-based key management KDC mainly on the logical level key scheme extensions such key management less processing method for the calculation of ordinary sensor nodes required, and does not require a lot of memory space Inter, the effective implementation of the first key to secrecy and backward secrecy, often use the method as HASH reduce the communication cost and improve the efficiency of key update "But in wireless sensor networks, usually KDC far away from the node, the node usually need to go through multiple hops to reach the KDC, therefore, expensive communications, lead to consume a lot of energy node.

3. Key Management and Security Policy of WSNs

Sensor network is composed of a large number of micro-sensors with sensing capability. Computing and communication capabilities have a network of systems. It allows people at any time. Any environmental condition detailed and reliable information. Therefore, the sensor networks in many areas there is a wide range of applications, but the sensor internet use is one of the largest military field. In this case, the authentication and key management and other security mechanisms secure communication between the sensor in the enemy area is very important, the key pre-distribution is the most basic sensor networks. One of the security mechanisms, which use passwords skills between the sensor nodes, can make secure communications, however, due to Energy restriction on the sensor node, the sensor using traditional key pre-distribution scheme. It is not feasible. If the data transfer for the user WSN is sensitive, then the secure communication of crucial WSNs important. Network security must have a realistic key management system as the basis, since WSNs compact node structure, capacity subject to many limitations, some of the classic traditional wired networks and wireless networks key management scheme, such as a Diffie Helman key exchange protocol, the key distribution center KDC (KDC: Key Distribution Center), RSA public key system, *etc*., does not apply in WSNs. First, WSNs are a distributed wireless network, and then rely on the deployment of collaborative work between the nodes end a task WSN nodes are embedded Micro Devices, does not exist in high-performance network server, You can't use the global key distribution center KDC to complete key management, and there can be no global public key infrastructure. Secondly, the biggest challenge facing the security WSN energy consumption as the representative to the RSA asymmetric public key algorithms use a lot of index calculation, which does not exist difficult for high-performance PC or workstations, but for the purposes of relatively low performance WSNs node is very difficult burden, the test results show that an asymmetric key algorithm for WSN does not apply.

2.1. Shared Key Management

There are two simple key pre-distribution scheme is a key pre-distribution scheme based on the probability of a special case, each one sharing a common node between the base station and a master key, the second is a master key is shared between each pair of nodes; In order to ensure communication between each node can directly use pre-shared key derived from the key encryption, the basic idea of the two programs as follows: the first program: This program for all nodes in a sensor network pre-assigned with a public master key, any pair of nodes communicate using the master key. The second scenario: The program requires that the sensor network between any pair of nodes using a different key communications "If the number of sensor network nodes N, each node to be pre-allocated N-1 different keys, named for the N-1 program, due to the communication key for any pair of nodes mutually different, in theory, the program allows the sensor network security to achieve the best performance. These two simple key pre-distribution scheme based on special circumstances random probability key pre-distribution scheme case, so that both the probability of secure connectivity between adjacent nodes P=1, and FIG key sharing under both scenarios will also be the complete graph, any two nodes can directly negotiate the shared key. However, these two simple the key pre-distribution scheme for the purposes of the sensor network is not realistic, the first program is very easy to implement now, but basically do not have security, so long as the master key leakage, the entire sensor network communications are disturbed whole. The second scenario requires that each node N a pre-assigned a key, the entire network needs to pre-allocate N*(N-1)/2 keys, since a large number of sensor nodes (N large), maintenance and management as this large key node for a very limited amount of storage resources and computing power is unrealistic, heavier the second solution is to not have the flexibility, because the dynamic

nature of sensor networks, you may need to dynamic changes in the network node, if the second option, to add a new sensor network node, new key distribution and negotiation will become very difficult.

2.2. Key Distribution Scheme

Basic random key pre-distribution scheme is proposed, aimed at prerequisite to ensure establishing a secure channel between any node to minimize resource requirements model node, the basic idea is that a relatively large key pool, pool any node has a key part of the key, just have a pair of identical keys between nodes can build safe passage, if the node key storage pool all key, the basic random key pre-distribution scheme degenerates to a point pre-sharing model, basic the specific implementation process random key pre-distribution scheme is divided into three main phases: (1) key pre-distribution phase, a key pre-distribution before node deployment is complete, system to construct a random key pre-pool, which contains the *S* mutually different key (*S* large), each key has a unique identifier "sensor network each node randomly selected from a pool m key keys stored in your of the EPROM ($m<S$), extracted key still however, back key pool, a process known as key distribution. (2) Direct negotiation shared key, after node deployment, and can be exchanged by neighbors to each other pre-shared key identifier to know whether a neighbor node has a public key. If two adjacent nodes have at least one public key, simply choose one of them as a shared key. "In this case, the key figure there is one shared between the two neighbors safe side, this process is called shared key direct negotiations. (3) Indirect shared key negotiation, if two adjacent nodes have no public key, and the third can have both with the public key as an intermediary nodes establish a shared secret key negotiation, this process is called shared key indirect negotiation, just make sure the key sharing graph connected graph, then any pair of adjacent nodes are available through direct or indirect party. Law Consultative establishes a shared secret.

2.3. Performance Analysis

A mathematical model program is random graph theory, random graph refers to the existence probability between any two sides of *p*, and *p* is a diagram of independent random variables equal probability, when $p=0$, the random graph has no edge, when $p=1$, the random graph is complete, random graph theory pointed out: If the number of nodes in a random graph is n, when n is large, if the whole random graph to become at least the probability P_r connected graph, there is the following limit formula:

$$P_r = \lim_{x\to\infty} P\left(G(n,p)_{con}\right) = e^{e-c} \tag{1}$$

Where *P* is the probability that any two points of communication, *C* is the specified threshold value, and there is a relationship-based

$$P=\ln(n)/n+(C/n) \tag{2}$$

When a given sensor network node number *n*, it had expected overall connectivity probability P_r, communication probability *P*, thereby to obtain an average degree d of the node.

$$P=(\ln(n)-\ln(\ln(P_r)))/n \tag{3}$$

$$d=P*(n-1) \tag{4}$$

Secure connectivity between probability P_r is the probability that neighbor nodes within its communication range communication security, and P is the probability of communication between any two points on the key shared diagram, sensor network node density as you can establish a link between the two, set sensor network deployment density *n* as an intermediary. Arbitrary node adjacent nodes Amount, according to the

number of nodes to ensure communication in random graph. The average degree d is large there is a limit to the fact that there is:

$$P_r=d/(n\text{-}1)=1\text{-}((S\text{-}m)!)^2/(S!(S\text{-}2m)!) \quad (5)$$

Since S is large, the formula may be used to simplify the factorial operation Stirling, (5) By the Stirling formula:

$$S!=\sqrt{2\pi}S^{S+0.5}e^{-n} \quad (6)$$

Simplified formula is as follows:

$$P_r=1\text{-}((1\text{-}m/S)^{2(S\text{-}m+0.5)})/((1\text{-}2m/S)^{(S\text{-}2m+0.5)}) \quad (7)$$

Equation (6), (7) gives the key pool size S, node number m pre-shared key and secure connectivity the relationship between the Pr. In general, for a specific deployment, the sensor network nodes number n, the overall probability of communication desired is constant, it is desirable that the average degree d is constant "and because the deployment density n. Usually is certain, it is desirable to secure connectivity probability P_r is a certain, according to the desired P_r can be set up meter suitable m and S, pre-shared key for each node number m is limited only by the size of the node storage resources, the key has nothing to do with the node resource pool size S, in FIG ensure key sharing communication conditions, the probability of more secure connectivity large more favorable, for which the key can be appropriately reduced the size of the pool, but the key is to reduce the pool to increase security in the communication takes while the rate of decline will lead to tolerance of security programs. After node deployment begins consultations identity shared key pre-distribution to all its neighbors broadcast keys characters, each node by broadcasting its neighbors know and how much they have the public key, the whole process is divided cloth style, because programs directly to a same public key as the shared key, the communication burden is not great. For the anti-attack capability scheme, we use quantitative indicators x nodes are the probability of capture, between a pair of nodes share uncaught 0 to assess key compromise. Since each node any probability of carrying a pre-shared key for m/S, so the x nodes are captured, not any pair capture probability between nodes shared key compromise is:

$$P_{conn}=1\text{-}(1\text{-}m/S)^x \quad (8)$$

2.4. Intrusion Detection of WSNS

The model number of the public key requirement was raised to q, q value can be increased to improve the resistance of the system force, attack network attacks and shared key number q difficulty exponentially. But in order to secure network the probability secure connectivity between any two points over q reaches the desired value p, we must reduce the size of the entire key pool, increasing the degree of overlap between the shared key nodes, but the key pool is too small the enemy will capture a few key nodes will be able to get a lot of space to find an optimal key pool size is the key to the implementation of this model.

Similar procedure extended random key pre-distribution model and basic model, just ask neighboring nodes public the key number is greater than the total of q, in access to all the shared key information later, if shared between the two nodes key number exceeds q, to q. A, then all q. Shared key generation with a key k, k=Hash($K_1||K_2||K_3\ldots||K_q$), as a shared master key between two nodes, Hash independent variable key sequence is pre-agreed specifications, so that the two nodes can calculate the same communication key.

$$P(i)=\frac{\binom{S}{m}\binom{S-i}{2(m-i)}\binom{2(m-i)}{m-i}}{\binom{S}{m}^2} \tag{9}$$

Where $P(i)$ for the extraction of m pre-assigned to the node from S keys, the two neighbors have an i, the probability of public keys, by the total probability formula, the two neighbors to establish a direct shared key is:

$$P_r=1-(P(0)+P(1)+\ldots.P(q-1)) \tag{10}$$

Almost the whole formula, when x nodes are captured, any pair the probability that an uncaught node shared key compromise is:

$$P_{conn}=\sum_{i=q}^{m}\left(1-\left(1-\frac{m}{S}\right)^x\right)^i\frac{P(i)}{P_r} \tag{11}$$

3. Key Implementation Process

This chapter describes the pre-shared key pre-distribution scheme model was improved, is proposed based on the node identifier symbol key pre-distribution scheme, this program is a probabilistic model, it does not store all n a key pair the shared key between the stores only a certain number of nodes to ensure that the probability of the safety communication between nodes p, thereby ensuring the security of network connectivity probability reach C, of the program have a good anti-trapping ability, since no shared key and space key pool, so even if the node captured, it will leak and its associated secret key and it is directly involved in the communication, and will not affect other nodes.

Random key pre-distribution scheme have shared key space and key pool, key space one of the biggest problems is the use of a large number of storage nodes in less than key information. The keys just build and maintain a secure channel secure channel when using the obtained "and the redundant information in the node captured when the attacker will provide a lot of sensitive information network, making the network node captured resist power is very low. Key pre-distribution scheme based on node identifiers, in order to configure the network nodes, we introduce node the concept identifier space, each storage node in addition to the key, but also correspond to the key store node identifier "When used in combination keys and node identifier to each node having a storage key local characteristics, meaning that all keys are for the node itself independently owned, with only the keys its paired node exists a "node so that if captured, it will only leak and its associated keys to and it is directly involved in communication, it does not affect other nodes. When the network node perceived when captured, you can notify their shared key nodes will be removed from the corresponding key on your key space from while greatly improving its anti-trapping ability, enhance network security, based on key pre-node identifier allocation of specific implementation process is as follows: (1) the initial stage arrangement. It is assumed that the maximum capacity of the network of n nodes, as possible n independent section. The only point distribution node identifier "actual size of the network may be smaller than n without node identifier in the new. The node is added to the network when used to improve network scalability. Assign a unique node identifier can be used to generate random number generator "random number generated by the random number generator is not only looks messy, but it should be from a nearly uniform distribution and context, irrelevant "So this random number can be used to make the network node identifier. Each node identifier m and another randomly selected to match the different node identifier, and each pair of sections point generates a key pair is stored in the nonvolatile memory of their "we can use the one-way hash algorithm standard method to generate a key assessment of the merits of a one-way hash algorithm has two:

one is the reverse operation function does not the presence or high complexity, avoid arguments by recovery result value; the other is the algorithm hair to a large absolute divergence, subtle changes in the independent variables can lead to completely different results, or difficult to find. The great similarity of its arguments are identical hash result, there is an equivalence argument is a hash conflict. The possibility is very small. (2) key discovery phase each node *i* broadcasts its first no to his neighbor, the neighbor nodes after receiving the broadcast packets from the ID, to see if a shared key to this node in the key ring on the as if there are, through the primary encryption handshake to confirm this and the other node does have shared key cases for example, between nodes A and B shared key, you can create between the completion of the exchange of information under the door key establishment:

$A \rightarrow *: \{ID_A\}$

$B \rightarrow *: \{ID_B\}$

$B \rightarrow A: \{ID_A | ID_B\} K_{AB}$, $\mathrm{MAC}(K_{AB}, ID_A | ID_B)$

$A \rightarrow B: \{ID_B | ID_A\} K_{AB}$, $\mathrm{MAC}(K_{AB}, ID_B | ID_A)$

After the handshake, the two sides confirmed node does have a common key between each other because node identifier is very short, so the communication overhead random identification key discovery process than previously described random key model small, and other random key pre-distribution of the same model, stochastic model also identifies key security topology the problem is not communication. This can increase the signal transmission power by not communicating nodes, in order to find more neighbors, increase the probability of a shared key with a neighbor node; it can be disconnected node with two or more hops node other than the key discovery process, a multi-hop fashion communication range of nodes expanded to alleviate. This can greatly increase the number of effective communication distance, in a safe neighbor node, thereby enhancing communication security probability, range expansion process should be gradually increased until the establishment of security connected graph up, multi-hop fashion extended range must be used with care, because the intermediate node during the packet forwarding and filtering no certification in the configuration stage, if an attacker sends packets to a random node, the data packet will be treated as positive. Often the key negotiation Packet replay many times in the network, this potential DoS attacks may be terminated or by slowing key establishment process, can be reduced by limiting the number of hops this method of attack on the network" as if the system of *D*, *S* attack sensitive, it is best not to use multi-hop feature" multi-hop process random key model, operation is not necessary. (3) key update stage, the key can't be static, communication key used for some time it is necessary to update the update key can be updated on the existing security link, but there is a risk suppose two nodes safety chain between road is established in accordance with the public key *k* between two nodes, according to the basic idea of random identification key model. We think, probably shared key *k* stored in other nodes in key ring. If your opponent captures some of the nodes, to gain the key *k*, and track all the key information for the entire time of the establishment, it can later obtain *k* solutions Encryption key update information to obtain a new communication key. (4) Nodes removal problems. Nodes removal process is mainly found in the failed node captured node or nodes to be copied when using the based key distribution model base is complete removal of the existing node via the base station, but since the node, and the base station communication delay is relatively large, this mechanism will reduce the rate of removal of the node in the removal process the malicious node must be cut off before it causes harm from the network, so rapid response is important.

Random identity key management model is a probabilistic model, it does not store all *n* a key pair, and shared key between the stores only a certain number of nodes to ensure

safe communication between nodes probability *p*, thereby ensuring the safety of the probability of network connectivity reaches *c* key identification number of nodes need to store the $m=n*p$ by the this formula can be seen, *p* smaller, the node needs to store key pair, the less so for random identification key models, to reduce the key storage node to the pressure, we need to secure communication in a given network to *C* under the premise of probability is calculated for a single node connectivity probability *p* minimum security even a single node security minimum pass probability *p* can be calculated as follows:

$$d=((n-1)/n)*(\ln(n)-\ln(-\ln(c))) \quad (12)$$

$$p=d/n \quad (13)$$

If a given node stores m random identification key, size of the network is capable of supporting as: $n=m/p$, according connectivity model *p*, *n* is relatively large in the case is likely to grow slowly *n* as m increases and p decreases and increases, the rate of increase depends on the network configuration model.

4. System Assessments

In order to verify the effectiveness and feasibility of the proposed method, if you take into account the key derived storage, the entire storage space for keys. It is a very huge number, and random node identification key model requires only a small amount of storage density key and a node identifier and can directly recognize the identity between the presence of any of the key pair node certificate, no other derived keys, so random logo node key model requires only a small amount of memory storage space, network size which can be directly supported by $n=m/p$ computing. Experimental data derived from the average of 50 times, Figure from 1 to 6:

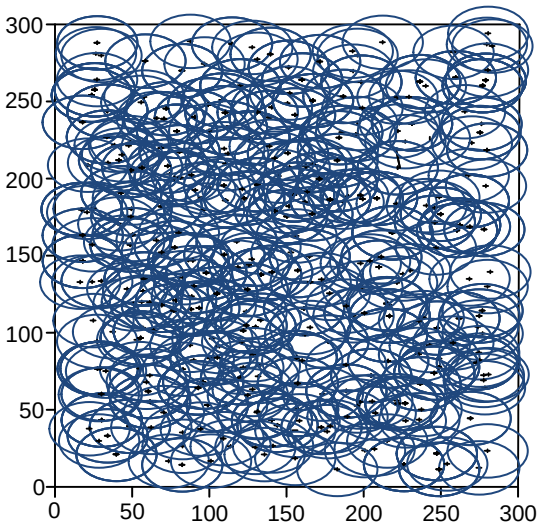

Figure 1. *t*=0, Initial Distribution of Nodes

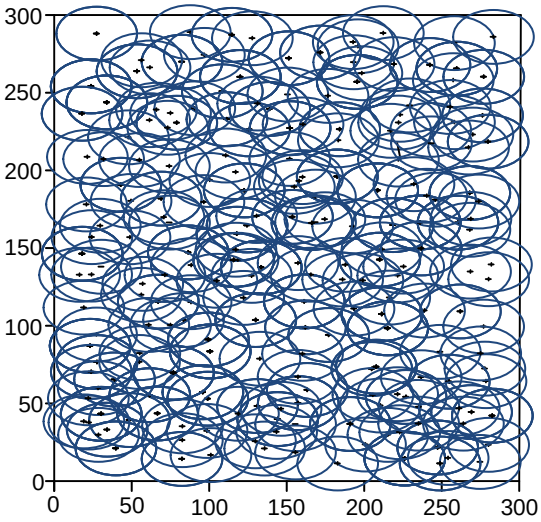

Figure 2. *t*=50, Nodes Deployment Optimization

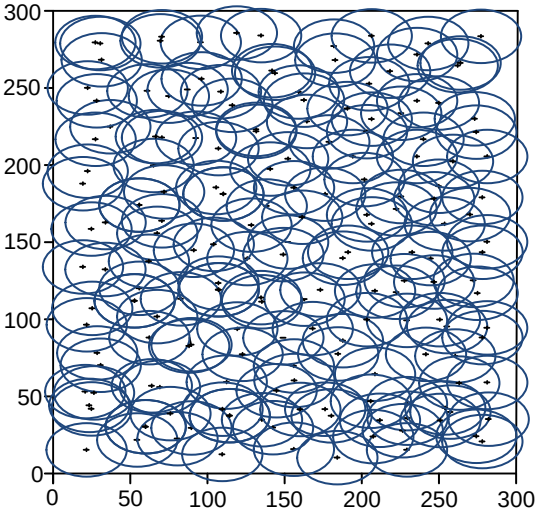

Figure 3. *t*=100, Nodes Deployment Optimization

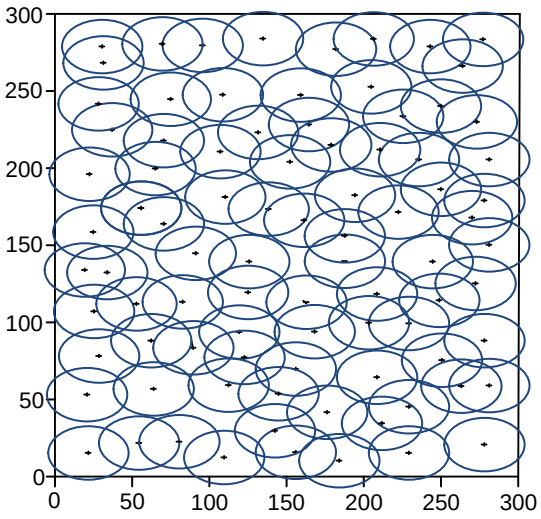

Figure 4. *t*=100, Nodes Deployment Optimization

Figures 1 to 4 are given the role at different time parameters, the sensor node deployment schematic initial time after deployment and text optimization. At *t*=0, the sensor nodes are deployed randomly in the form of high density, can be seen from Figure 1, there are a large number of redundant nodes 300*300m^2 monitored area; over time, under certain coverage of the premise, according to the relevant formula to calculate the expected value of each time covering the monitoring area, close the corresponding redundant nodes to improve overall network security.

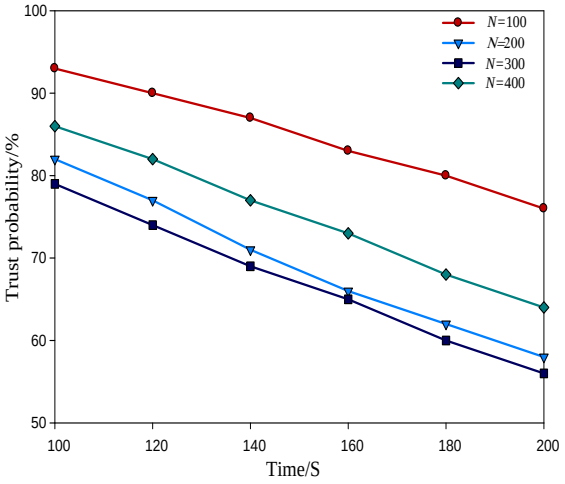

Figure 5. Simulation Model Contrast

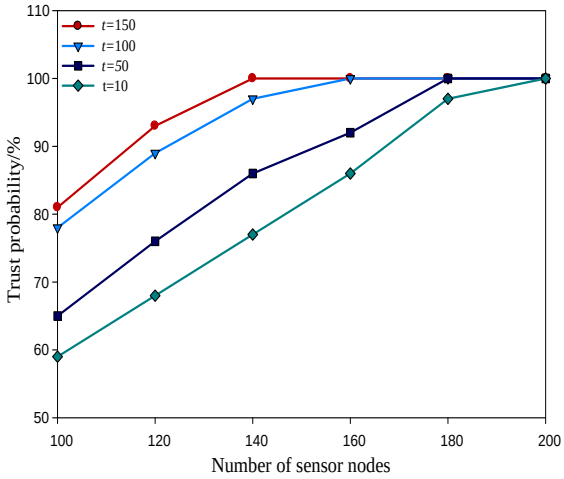

Figure 6. Number of Different Nodes of Simulation Model

Through ten randomly generated set of data as the source data to simulate the 100 nodes directly credit parameters, energy parameters and indirect credit parameters, the results shown in Figure 5. Although higher values can be seen by some nodes credibility reputation model calculated indicating that the communication behavior of nodes is credible, but chance nodes in the network is longer or selected to perform tasks more credibility resulting in lower its energy value, calculated based on the credibility of the node behavior model calculated Comprehensive credit reputation value calculated low value, and therefore the calculation model based on the credibility of the node acts reputation management system can be integrated to judge the credibility of the lower value of the node and reduce the chance of it is selected to perform the task, thereby extending its life cycle, reflect the fairness of the network. Suppose node *j* to node *i* totally credible, whereby node *j* credit rating the results are shown in Figure "With increased node *i* and node *j* successful transactions 6, node *i* the calculated value of the node *j* directly assess the credibility of the increasingly high, tended to 1, meaning in terms of the credibility from the direct node *j* is more credible. But if the credit in calculating indirect communication node k as its credibility credit rating, the node *k* if it is malicious nodes can exchange for a higher credit rating through reliable communication behavior, by comparing to the node *j* low indirect reputation to denigrate node *j*, resulting in a lower node *j* at node *i* credibility, can't even letter, but the credibility of the evaluation terms of reference node *k* to evaluate the behavior of *k* words, when *k* credible evaluation of behavior, it is also to evaluate the credibility *j* closer to real transactions, calculated from the node *i* node *j* directly Fully reputation and credibility of the indirect combined high value, reflecting the behavior of trusted nodes *j*.

5. Conclusion

This paper introduces the application prospect of wireless sensor networks, wireless sensor systems elaborated network theory and technology, focusing on wireless sensor network security features and the various aspects of off key technology, especially for a variety of wireless sensor networks key management scheme in-depth study and based on the design of a key pre-distribution scheme based on node identifier, the program has a strong anti-Trapping ability, thereby effectively raising the sensor network security.

Acknowledgments

Project (14B520099, 16A520063) supported by Henan Province Education Department Natural Science Foundation; Project (142102210471, 162102210113) supported by Natural Science and Technology Research of Foundation Project of Henan Province Department of Science.

References

[1] Z. Liu, Y. Hu and X. Zhang, "Certificateless signcryption scheme in the standard model", Information Sciences., vol. 18, no. 3, **(2010)**, pp. 452-464.
[2] Z. Eslami and N. Pakniat, "Certifiateless aggregate signcryption: security model and a concrete construction secure in the random oracle mode", Journal of King Saud University Computer and Information Science., vol. 26, no. 3, **(2014)**, pp. 276-286.
[3] J. Kar, "Parovably secure on-line off-line identity-based signature scheme for wireless sensor networks", International Journal of Network Security., vol. 15, no. 6, **(2013)**, pp. 411-421.
[4] Z. Wang and W. Chen, "An ID-based online/offline signature scheme without random oracles for wireless sensor networks", Personal & Ubiquitous Computing., vol. 17, no. 5, **(2013)**, pp. 837-841.
[5] J. K. Liu, J. Baek and J. Zhou, "Efficient onling/offline identity-based signature for wireless sensor networks", International Journal of Information Security., vol. 9, no. 4, **(2010)**, pp. 284-296.
[6] F. G. Marmol and G. M. Perez, "Providing trust in wireless sensor networks using a bio-inspired technique", Telecommunication Systems., vol. 46, no. 2, **(2011)**, pp. 163-180.
[7] L. Gu, Y. Pan and M. Dong, "Noncommutative lightweight signcryption for wireless sensor networks", International Jouranl of Distributed Sensor Networks., vol. 13, no. 1, **(2013)**, pp. 1-10.
[8] C. Hu, N. Zhang and H. Li, "Body area network security: A fuzzy attribute-based signcryption scheme", IEEE Journal on Selected Areas in Communications., vol. 31, no. 9,**(2013)**, pp. 37-46.
[9] X. Fan and G. Gong, "Accelerating signature-based broadcast authentication for wireless sensor networks", Ad Hoc Networks., vol. 10, no. 4, **(2012)**, pp. 723-736.
[10] J. Zhang and V. Varadharajan, "Wireless sensor networks key management survey and taxonomy", Journal of network and computer applications., vol. 33, no. 2, **(2010)**, pp. 63-75.
[11] R. P. Lakshmi and A.V. Kumar, "A fuzzy based secure QoS routing protocol using ant colony optimization for mobile ad Hoc networks", Journal of Intelligent and Fuzzy Systems., vol. 27, no. 1, **(2014)**, pp. 317-329.
[12] S. H. Lee, S. J. Lee and K. I. Moon, "A combined system of secure hashing and neural networks in sensor networks of living environment", International Journal of Control & Automation., vol. 7, no. 9, **(2014)**, pp. 55-66.
[13] B. Kadri, M. Feham and A. Mhammed, "Efficient and secured ant routing algorithm for wireless sensor networks", International Journal of Network Security., vol. 16, no. 2, **(2014)**, pp. 149-156.

Authors

Zeyu Sun, He was born in 1977 in Changchun city, Jilin Province, in 2009 graduated from Lanzhou university, Master of Science; Xi'an Jiaotong university study for Ph.D at present. He is associate professor in School of Computer and Information Engineering, Luoyang Institute of Science and Technology, and is also a member of China Computer Society. The main research interest is in wireless sensor networks, parallel computing and Internet of things.

Longxing Li, He was born in 1966 in Jiaozuo city, Henan Province, in 2009 graduated from University of Science and Technology Beijng, Ph.D. He is professor in School of Computer and Information Engineering, Luoyang Institute of Science and Technology. The main research interest is in wireless sensor networks and Internet of things.

Xuelun Li, (1995-) She was born in Luoyang City, Henan Province. School of Electronic information Engineering, Tianjing University. The main research interest is in wireless sensor networks, parallel computing and Internet of things.