Sensors & Transducers, Vol. 160, Issue 12, December 2013, pp. 323-328

www.sensorsportal.com

Sensors & Transducers

http://www.sensorsportal.com

On Application of the Security of Wireless Sensor Network Data to Digital Library Information Service-Based on Agent Model

Xin LIU

Economics and Management School of Wuhan University
Room 707, No. 78 Dong Ge Road, Nanning, Guang Xi, China 530022
Tel.: 86-771-2282839, 86-13807888808, fax: 86-771-2282856
E-mail: liuxinx12@163.com

Received: 2 November 2013 /Accepted: 22 November 2013 /Published: 30 December 2013

Abstract: This paper aims to study the application of the security of wireless sensor data to the digital library services. Take the user's personalized information need as the research object and build the Agent model. Combined with the user preference model, build multivariate function and put forward region-based secret key pre-allocated protocol. Using deployment knowledge to increase the probability of shared key and design an identity-based dynamic multiple-cluster key management model which elaborates respectively personalized information acquisition, analytic processing and delivery process. Draw a conclusion: With the introduction of regional information, can solve the security problems of conspiracy attack of combination of public key cryptography under certain conditions. By introducing the security of wireless sensor network data into the digital library, tracking of information resources can be more safe and effective and the optimization of user information needs is thus realized. *Copyright © 2013 IFSA.*

Keywords: Wireless sensor; Agent model; Digital library.

1. Introduction

Wireless sensor network [1] is a multi- hop self-organizing network formed by a large number of low-cost micro sensor nodes deployed in monitoring area through wireless communication mode. Collaboratively percept, collect, process and transmit perceived object information in network coverage area and finally send this information to network owners. Initially, the wireless sensor network is applied in the military field. At present, wireless sensor network has achieved good development in many business fields. Such as health care, home automation, environmental change monitoring and traffic control and so on. Personalized information service of digital library based on the characteristics of user's interests and hobbies, take the initiative to provide users the information which meet their individual needs. Wireless sensor network data security technology is applied to digital library to improve the quality of personalized service, and some confidential information can be delivered more safely. To achieve the high efficiency and high quality service, some technical support is needed. Agent is used to design the personalized service model for the library, which can well solve the problem. This model can actively search, analyze, choice and recommend information for users according to their special requirements. A more targeted, user-oriented personalized service

mechanism is established. It reflects a user-centered service that make the library developed from passively provide information for reader to actively seek knowledge for them, so as to improve the utilization of library resources.

Many scholars at home and abroad have done researches on individualized information service of digital library. For example, My Library system [2] of Cornell University which includes three service contents of Mylinks, Myupdates and MyContents [3] on personalized push service and development of push system of digital library. In China, "my library" system developed by Zhejiang university library includes functions such as bookmarks, custom library digital resources, the latest information announcement, search engine links, custom WEB page style, etc. For the study of personalized information recommendation service, typical foreign research projects are: ihrrnina, Cite, Seer and Fab. At home, there is a "Digital library personalized recommendation system" co-developed by school of information, Renmin University of China and its library. This paper adopts the intelligent Agent to design library personalized service model which is user-centered. Study under the Agent model, the operation principle and function of information collection, analytic processing and push links of digital library. Finally, it put forward that personalized information service system development cannot do without technical support of other disciplines, it should be viewed as a comprehensive solution.

2. Research Design

2.1. Theoretical Basis

2.1.1. Agent Model

Agent is a concept developed in the field of artificial intelligence (AJ), it is a software entity which automatically collects information according to user requirement and transmits it to the designated location according to the specified way by the user. It has many kinds of ability, such as the ability to perceive the external environment, problem solving skills and the ability to communicate with the outside world, etc. The Agent technology is originally a branch of distributed computing and it is widely used in commercial, manufacturing, finance, e-commerce and other fields. Because it can continue to play a role independently, so it becomes the intermediary agent of the contact between users and information resources.

2.1.2. Wireless Sensor Network

Wireless sensor network [1] is a multi- hop self-organizing network formed by a large number of low-cost micro sensor nodes deployed in monitoring area through wireless communication mode. Collaboratively percept, collect, process and transmit perceived object information in network coverage area and finally sends this information to network owners.

2.2. Build Up of Model Agent

Abstract Agent model can be expressed as: Ag:RE→Ac, the external environment condition set is: E={e, e', …}, Agent movement set is: Ac={a, a', …}, R is a perform collection of E and Ac state change. The model is a closed loop system. First of all, according to the change of perceive environment state, map execution to the movement. Then, output motion is acted on environment, the specific process is shown in Fig. 1.

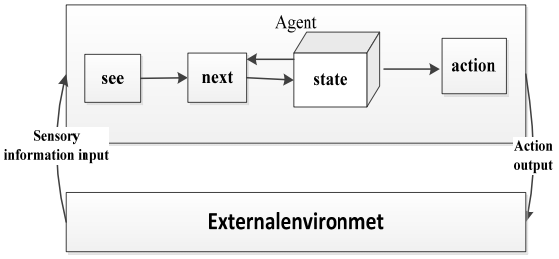

Fig. 1. Agent abstract model.

Agent starts from the initial internal state i_0, observes external environment condition e and creates a cognitive function $see(e)$. Then updates the Agent's internal state by function next to $next[i_0, see(e)]$, and compares with the state library. Agent selects a perform action r through $action\{next[i_o, see(e)]\}$, and r presents an alternating sequence between environmental state e and a:

$$e0 \xrightarrow{a_0} e1 \xrightarrow{a_1} e2 \xrightarrow{a2} \cdots \xrightarrow{a_{u-1}} eu,$$

a is action subject. After action execution, Agent backs to the source and perceives information input of the external environment. Next updates the input information and perform the action finally, to complete a new cycle again.

3. Empirical Analysis

3.1. Region-based Random Key Pre-distribution Scheme

This scheme is based on random key pre-distribution scheme and is divided into three stages with first stage using regional information, the

second and third stage using random key pre-distribution scheme.

3.1.1. Secret Key Pre-distribution Stage

Before the deployment of sensor nodes, key pre-distribution should be carried out first. First of all, coverage area of wireless sensor network should be divided into several regions, domain (i, j), then the network manager generates key pool S, in order to make each region corresponds to a key pool, S is also divided into same number of sub key spaces, subset (i, j). And overlap factor c represents the proportion of sub-key overlaps on sub-key space between adjacent domains. By this time, node selects randomly m number of different keys as its secret keys in the corresponding sub-key space. When the wireless sensor network coverage area is not divided, the scheme is equivalent to random key pre-distribution scheme. Otherwise, if the quantity of the divided areas is big enough, i.e. one sensor node corresponds to one region, then the scheme degenerates to the location situation before the deployment of each nodes.

Assuming the sub-key space corresponds to one area of the wireless sensor network domain (i, j) is: subject (i,j), and A(x,y) and B(x',y') represents respectively the sub-key space, subject (i, j).

The coordinates of the element A and B can be calculated through the following equation.

$$\begin{cases} x = \dfrac{1-c}{M-(M-1)\cdot c}\cdot i\cdot(M\times r) \\ y = \dfrac{1-c}{N-(N-1)\cdot c}\cdot j\cdot(N\times r) \end{cases},$$

$$\begin{cases} x' = \dfrac{(1-c)\cdot i+1}{M-(M-1)\cdot c}\cdot(M\times r)-1 \\ y' = \dfrac{(1-c)\cdot j+1}{N-(N-1)\cdot c}\cdot(N\times r)-1 \end{cases},$$

In the equation, M and N represents that wireless sensor network is divided into M×N regions. c is the overlap factor of adjacent domains. r is the key matrix coefficient.

By the theory of random graph, quantitative relation between node number N, mean nodal degree d and global connectivity probability Pc should meet the following equation:

$$d = \frac{N-1}{N}\left[\ln(N)-\ln(-\ln(Pc))\right],$$

If the wireless sensor network (WSN) wants to arrive a specific global connectivity probability Pc, then communication radius R, average neighbor node number D, local connectivity probability between two nodes P_{local} must meet the following equation:

$$P_{local} = \frac{d}{D-1} = \frac{1}{D-1}\frac{(N-1)}{N}\left[\ln(N)-\ln(-\ln(Pc))\right]$$

If wireless sensor network is not divided, and the total size of the key pool is s, each node saves m number of keys. Then probability P_{share} of at least one share key between any two nodes in a network must meet the following equation:

$$P_{share} = 1-\frac{((s-m)!)2}{s!(s-2m)!}$$

Therefore, if RKPS scheme is required to meet the global network connectivity probability Pc, it must meet the condition: $P_{share} \geq P_{local}$.

If the wireless sensor network is divided into M * N sections of the same size, and node's key chain are randomly selected from the corresponding key space, the probability of two nodes in the same area share a key is represented by P1, the probability of two nodes share a key between adjacent areas is represented by P2, the following can be obtained:

$$P1 = 1-\frac{\left(\left(\frac{w}{c}-\frac{\tau}{c}\right)!\right)^2}{\left(\frac{w}{c}\right)!\left(\frac{w}{c}-2\frac{\tau}{c}\right)!},$$

$$P2 = 1-\frac{((w-\tau)!)^2}{w!(w-2\tau)!},$$

In the equation,

$$w = \frac{c\cdot s}{\left[M-(M-1)\cdot c\right]\left[N-(N-1)\cdot c\right]},$$
$$\tau = m\cdot c, c$$

where c is the overlap factor; s is the size of the key pool, m is the key chain length of the nodes.

3.1.2. Shared Secret Key Discovery Stage

After the nodes are assigned to the designated area according to the demand, it comes to the second stage-shared secret key discovery stage. Assume S for key pool, K for the key, because in the last stage, the nodes have acquired their own key chain. There is m number of keys in each of the key chain and each key has a unique identifier. In this stage, the shared secret key can be found through the following two methods:

1) Broadcasting method. Because each key has a unique identifier, the nodes can broadcast the m number of identifiers which belong to them. If same

identifier is found in neighbor nodes, it means that there exists a shared key between the two nodes.

2) Nodes encrypt the key identifiers $\alpha, E_{K1}(\alpha), E_{K2}(\alpha), \cdots, E_{Ki}(\alpha), \cdots, E_{Km}(\alpha)(i = 1,2,3,\cdots,m)$, then broadcast them out, α is a random number, E_{Ki} represents information after encryption. Accordingly, in order to determine whether there is a shared key between nodes, neighbor nodes will also make same encryption operation to α by their own key. If there exists a same shared key, it is used as the session key between two nodes in the future.

3.1.3. Path Key Establishment Stage

After finishing the shared secret key discovery phase of wireless sensor network, it can be viewed as a shared secret key figure G（V, E）, V represents the nodes that share a key with their neighbor nodes. E represents a secure link between the nodes.

In order to ensure the data security, inter-node communication needs to use communication keys. However, if there is no shared key between one specific node and its neighbor node, other ways are required to negotiate the session key between nodes. In order to let the persistence ration of figure G (V,E) reaches the requirement of global connectivity Pc, the key pre- distribution phase must meet the condition: $P1 > P2 > P_{share}$. Suppose G (V,E) is a connected graph, by the definition of a connected graph, a communication path can be found between any two neighbor nodes.

3.2. Agent Personalized Information Acquisition Process

The key of personalized service is the acquisition of the user dynamic information. There are two ways for intelligent Agent information acquisition: One is regularly polling Web log and collect user information on a regular basis. The second is the Agent real-time tracking. Timely action is taken once changes are found and user's personalized information is analyzed. The specific process is shown in Fig. 2.

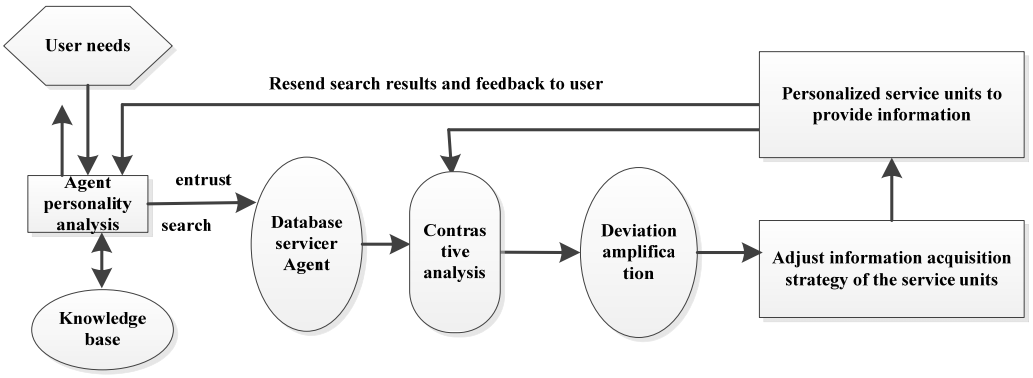

Fig. 2. The Agent personalized information acquisition process.

According to user requirements, Agent makes character analysis and contacts all database which may possibly store user information needed, entrust them to find information that matches the model. Through the knowledge base rules, reasoning judgment is made and personalized information service is extracted. Then return the search results back to Agent. Finally adjust the weights of reasoning algorithm of the knowledge base, and after the search results are cleared up, they are feedback to the user.

3.3. Processing Procedure of Agent Personalized Information Analysis

Personalized processing module is the core of the whole system and it is responsible for the normal operation of the whole system. It makes personalized analysis and processing of needs of users, refines personalized information contents and translates them into the information which can be identified by machines. Its structure is shown in Fig. 3.

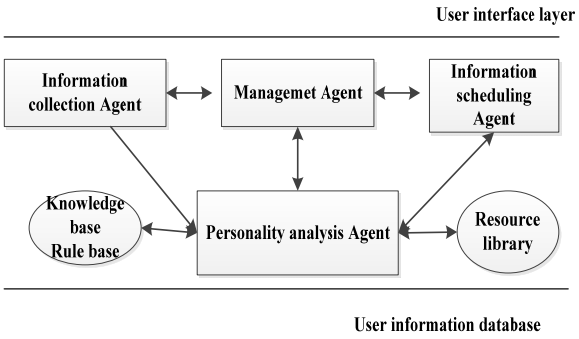

Fig. 3. Processing procedure of Agent personalized information analysis.

The Agent mainly collects data from subscriber interface module and simple classification is carried on. After the information is gathered, they will be sent to the personality analysis Agent group.

3.4. Agent Personalized Information Push Process

Push module's main function is to feedback information to the user after recommendation module processing based on the previous system information. This paper through the establishment of user preference model, studies the push process of personalized information of digital library. Based on the model characteristics, 3 yuan equation set is established: $P: P=(M,F,\psi)$. Of which,

$$M=\left\{M^{(0)},M^{(1)},\cdots M^{(M)},\cdots M^{(n)}\right\},$$

$$F=\left\{F^{(1)},F^{(2)},F^{(M)},\cdots F^{(n)}\right\},$$

$$\psi: M\times F\to M,\left\{M^{(M+1)}=\left(\psi^{M(i)},F^{(i+1)}\right),i=0,1,\cdots,n\right\},$$

Here, M is the all state set generates in the system using process. F is the all feedback information set collected, with its role to drive the update process. ψ is renewal function.

$M^{(0)}$ reflects the initial state of the user model. $M^{(i)}$ is user preference model after i number of update. $F^{(i)}$ is the information used for updating $M^{(i+1)}$ with i number of feedbacks to the system. The formalized description reflects the user preference model in the system is in a state of constant updates and synchronously reflects the user's preferences.

According to the user object characteristics of the digital library recommender system, this paper puts forward the organic combination of considering long-term and short-term preferences of users. Set the preferences based on their age, professional background, education level, etc, as the long-term preferences. Make Inquire records of the user's preference classification and sample documents, the preferences based on this analysis is set as short-term preferences. When finally considering user preferences tendencies, we determine a preference model such as $\alpha M^L+(1-\alpha)M^S$, M^L is a long-term preference feature vector, M^S is a short-term preference feature vector, α is a parameter to adjust incidence between long-term and short-term preferences. Its taking value interval is $(0\sim 1)$.

Make a formal description of the classification system T as a tree structure, $T=(C,R)$, of which, $C=\{c1,c2,\cdots,ci,\cdots cn\}$, is a collection of all categories which belongs to that classification system. ci is the No i. category of C. $R=R=\{\langle ci,cj\rangle\in r|1<i<j<n\}$, is the hyponymy between the classifications. $|\langle ci,cj\rangle\in r$ represents that classification ci is the parent class of cj.

By rule-based reasoning, it can be learned that the users may be interested in some classifications, for example, ci,cj,ck and so on. Which is corresponding to $\{ct1,ct2,\cdots,cti,\cdots\}$ of ci. The result M^L can be denoted by:

$$\begin{aligned}M^L&=ci\cup cj\cdots\cup ck,\\&=\{ct1,ct2,\cdots,cti,\}\cup\{ct'1,ct'2,\cdots,ct'i\}\cup\\&=\{ct1,ct2,\cdots cti,\cdots ct'1,ct'2,\cdots ct'i\cdots\}\end{aligned}$$

However, sometimes the user's choices may be more than one category. For this kind of situation, when user preference model is set up, two situations need to be considered that whether the user preference classification is a child-parent classification or a peer classification. When the user selects multiple preferences classification, initial user preferences model M^S is denoted by:

$$\begin{aligned}M^S&=\alpha ci\cup\beta cj,\\&=\alpha\{ct1,ct2,\cdots cti,\cdots\}\cup|\beta\{ct'1,ct'2,ct'i,\cdots\}\\&=\{\alpha ct1,\alpha ct2,\cdots,\alpha cti,\cdots\beta ct'1,\beta ct'2,\cdots\beta ct'i,\cdots\}\end{aligned}$$

α,β is the weight, represents respectively the preference degree of the peer categories.

Set an attenuation factor $\gamma(0<\gamma<1)$, to represent the changes of subclasses, as follows:

$$\begin{aligned}M^S&=\alpha\gamma\{cj|\langle ci,cj\rangle\in r\}\cup\beta ci,\\&=\{\alpha\gamma ct1,\alpha\gamma ct2,\cdots,\alpha\gamma cti,\cdots\beta ct'1,\cdots,\beta ct'i,\cdots\}\end{aligned}$$

Agent technology services can not only transfer information to users, when the conditions are met, it can timely and actively push constantly updated dynamic information to users according to the information characteristics and sending requirements pre-set by the users when the network information is updated, and let users grasp the latest information. Personalized information service applies intelligent Agent search engine technology, comprehensively mining and collecting user's interests and making automatic analysis and recognition of the information according to the specific information requirements or template set by users. And transmit the filter results which meet user requirements to users by the specified way of the user, so as to realize the cycle operation of the entire service system.

4. Conclusion and Discussion

4.1. Conclusion

From the above analysis, the following conclusions can be obtained:

Digital library personalized information system is mainly made up of three modules. There is close relation between each module and a complete relation chain is formed.

With the introduction of regional information, on the basis of random key pre-distribution scheme, put forward region-based key pre-distribution scheme of wireless sensor network. The simulation results show that the performance of the scheme is better than random key pre-distribution scheme.

In terms of theoretical research and technological realization, Internet oriented digital library individualized active information service is a multidisciplinary cross system engineering, which needs an integrated application of a variety of theories and technologies such as information retrieval, artificial intelligence, data mining and so on.

4.2. Discussion

Open and broadcast characteristic of wireless sensor network deployment area both make it face potential safety hazard. Wireless sensor network and traditional network have the same security requirements. However, due to its resource constraint, traditional security technology can not be directly applied to wireless sensor network. Complicated application environment requires higher safety and efficiency for wireless sensor network. Therefore, how to design a safe and efficient scheme has become the future research focus of the subject.

References

[1]. W. Guang, Theoretical and experimental research on wireless sensor network node location technology, *Huazhong University of Science and Technology*, 2013.

[2]. Z. Qiang, Based on the connectivity of wireless sensor network node location technology research, *Tianjin University,* 2011.

[3]. L. X. Shuamg, Wireless sensor network node security positioning research, *Hebei Normal University*, 2012.

[4]. Z. Yufeng, Y. Chuangye, Individualized information service model study based on Agent, *Journal of Intelligence*, Vol. 05, 2010, pp. 56-59.

[5]. L. Yongxian, Z. Pengwei, Personalized information push service model study based on Agent, *Information Technology*, Vol. 07, 2011, pp. 55-58.

[6]. H. Xiquan, Modeling method on user preference of digital library recommender system, *Intelligence Methods*, 01, 2006, pp. 28-29.

[7]. Chen Xiulian, Application of Agent personalized intelligent information retrieval system on the science platform of digital library, *Science and Technology in Western China*, Vol. 01, 2008, pp. 94-96.

[8]. L. Xiaoyong, Realization of personalized information service based on Agent technology, *Library Journal*, Vol. 04, 2006, pp. 127-128.