2016

Supporting Business Privacy Protection in Wireless Sensor Networks

Nan Feng

Zhiqi Hao

Sibo Yang

Harris Wu
Old Dominion University, hwu@odu.edu

Original Publication Citation

Feng, N., Hao, Z. Q., Yang, S. B., & Wu, H. (2016). Supporting business privacy protection in wireless sensor networks. *Journal of Sensors, 2016*, 7638149. doi:10.1155/2016/7638149

Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 7638149, 11 pages
http://dx.doi.org/10.1155/2016/7638149

Research Article

Supporting Business Privacy Protection in Wireless Sensor Networks

Nan Feng,[1] Zhiqi Hao,[1] Sibo Yang,[1] and Harris Wu[2]

[1]*Department of Information Management, Tianjin University, Tianjin 300072, China*
[2]*Old Dominion University, Norfolk, VA 23529, USA*

Correspondence should be addressed to Sibo Yang; yangsibo@tju.edu.cn

Received 15 March 2016; Revised 19 May 2016; Accepted 21 June 2016

Academic Editor: Jose M. De Fuentes

With the pervasive use of wireless sensor networks (WSNs) within commercial environments, business privacy leakage due to the exposure of sensitive information transmitted in a WSN has become a major issue for enterprises. We examine business privacy protection in the application of WSNs. We propose a business privacy-protection system (BPS) that is modeled as a hierarchical profile in order to filter sensitive information with respect to enterprise-specified privacy requirements. The BPS aims at solving a tradeoff between metrics that are defined to estimate the utility of information and the business privacy risk. We design profile, risk assessment, and filtration agents to implement the BPS based on multiagent technology. The effectiveness of our proposed BPS is validated by experiments.

1. Introduction

Wireless sensor networks (WSNs) are highly distributed networks that are enabled with wireless communication technologies and composed of devices with sensing capabilities [1, 2]. The rapid development of WSNs is changing the way people live and work. Extensive research has focused on a broad range of applications of WSNs, including both the military and civilian domains [3, 4]. However, it is the issue of privacy protection that has drawn considerable attention from the research community. This is because of the implementation of WSNs in commercial scenarios involving businesses and individuals.

Privacy protection has been studied in many fields associated with the applications of WSNs. Nevertheless, the following inherent characteristics lead to some challenges for privacy protection in WSNs.

(i) Uncontrollable environment: sensors are commonly employed in an environment without sufficient security control.

(ii) Resource constraints: the ability of a sensor node to store, process, and transmit the sensed data is generally limited by its power supply.

(iii) Topological constraints: due to the limited communication range of sensor nodes, multiple hops are required for transmitting data. Such a transmission scheme may cause an unbalanced network load.

In addition to the above challenges, employers must pay much attention to the threat of business privacy leakage due to the accessibility of WSNs [5, 6]. The attributes of WSNs may lead to the disclosure of sensitive information regarding the enterprise. This is susceptible to being collected and analyzed by an adversary, who can in turn harm the enterprise's business privacy [7]. Thus, when an enterprise employs a WSN for commercial transactions, the disclosure of sensitive or confidential information will be inevitable without effective business privacy protection.

Although business privacy protection is imperative in the applications of WSNs, there has been minimal attention devoted to the threat of business privacy leakage for enterprises. Existing studies focus mainly on how to protect the individual's privacy in the context of WSNs [8–11]. Therefore, in this paper, we propose a business privacy-protection system (BPS) that is designed specifically for enterprises in order to reduce the threat of business privacy leakage in WSNs. The BPS is implemented by three types of agent:

a profile agent, a risk assessment agent, and a filtration agent, all based on multiagent technology. Integrating the current risk level of privacy leakage, the BPS makes a tradeoff between the utility of information transmitted in a WSN and the risk of privacy leakage and finally generates the optimal filtered profile that satisfies the security requirements.

The remaining sections of this paper are organized as follows. We first review the relevant literature. Then, Section 3 presents the components of our proposed BPS in detail. In Section 4, the BPS is validated further by extensive experiments. Finally, we summarize our contributions.

2. Literature Review

Privacy protection in WSNs can be categorized as data-oriented and context-oriented [12]. Data-oriented privacy protection focuses on protecting the privacy of the data sensed by the nodes [13] and the queries posted to the WSN [14]. Context-oriented privacy protection focuses instead on protecting the metadata related to the transmission of data, such as the information of time and location. This paper aims at solving the issues in data-oriented privacy protection.

To understand the challenges of privacy protection in WSNs, it is necessary first to review the privacy issues and privacy-protection approaches as follows.

Privacy concerns related to sensed-data management have been proposed in several different systems [15]. (1) Data-collection system: the privacy-protection methods commonly employed in data-collection systems are random-perturbation techniques [16, 17]. (2) Information-sharing system: such systems commonly use cryptographic secure multiparty computation techniques [18, 19]. (3) Data-publishing system: the system's purpose is to facilitate data-analysis applications. In these systems, algorithms based on k-anonymity [20] and l-diversity [21] are widely used to protect privacy. Privacy issues have also been investigated in privacy-protection schemes. In [22, 23], the researchers emphasized that the sender's location information is the most important data that need to be protected. Some researchers have tried to hide the origin of the message [24]. Mehta et al. [25] first focused on the location privacy of sensor networks in the global environment, the assumption which became the basis for future research. In order to protect the location privacy, some scholars proposed a new approach for network topology discovery that allows the sink to obtain a global view of the topology without revealing its own location [26]. Some scholars addressed the importance of location privacy of both the source and sink and proposed four schemes, respectively, to deliver messages from source to sink, which can protect the end-to-end location privacy against local eavesdropper [27]. In order to resist the attacks targeted at the base station of WSNs, some scholars present HISP-NC (Homogenous Injection for Sink Privacy with Node Compromise Protection), a receiver-location privacy solution that consists of two complementary schemes which protect the location of the base station [10].

In recent years, multiagent technology has been widely applied in the field of privacy protection. A multiagent system (MAS) is a system consisting of several agents. Agents coordinate among the various members, provide service for one another, and together complete a task. The goal of a MAS is to convert large and complex systems into small, well-communicated, well-coordinated, and easy-to-manage systems [28]. In a MAS, each agent is independent, autonomous, and able to solve a given problem. Simultaneously, it is a coordinated system in which agents solve large complex problems in coordination with one another. As for the privacy protection related to privacy leakage, some researchers have focused on a secure model that shows how to maintain the secrecy in a cloud environment by using a MAS. Yang et al. [29] focused on developing an active defense for emergency-management system engineering using a MAS. Bishop et al. [30] proposed a mobile agent-based approach to automate the process of detecting and monitoring a colored file system for privacy protection. In this paper, we utilize multiagent technology to build our proposed BPS. There are three agents, profile, risk assessment, and filtration agents, that interact with each other for the common goal of privacy protection in a WSN.

In this paper, we examine the business privacy protection in a WSN. We model the sensed information as a hierarchical profile. Furthermore, we utilize multiagent technology to build our proposed BPS. There are three agents, profile, risk assessment, and filtration agents, that interact with each other for the common goal of privacy protection in a WSN. In the filtration agent, a filtration is developed to filter sensitive information from the profile with respect to enterprise-specified privacy requirements. In addition, the effectiveness and the scalability of the filtration are validated by experiments.

Table 1 shows the comparison results between our proposed BPS and other widely used three approaches, namely, DCARP [26], FRW [27], and HISP-NC [10], where NA means information not found in the related references.

The first issue is the capability of risk level evaluation. In WSN, the entire system faces many risks, and we need to assess the risk and determine the risk level that the enterprise is now facing. As a result, it can be determined which appropriate measures need to be taken immediately to reduce the risks. In BPS, based on BN, we can analyze the current risk level of the enterprise. The second issue is about the information filtration. Faced with the risk, enterprise must

Table 1: Comparison between BPS and other approaches.

	BPS	DCARP	FRW	HISP-NC
Risk level evaluation	Yes	No	No	No
Information filtration	Yes	No	No	No
Location privacy protection	Yes	Yes	Yes	Yes
Resisting traffic analysis	No	Yes	No	Yes
Tool support	Hugin expert	NA	TOSSIM	MATLAB

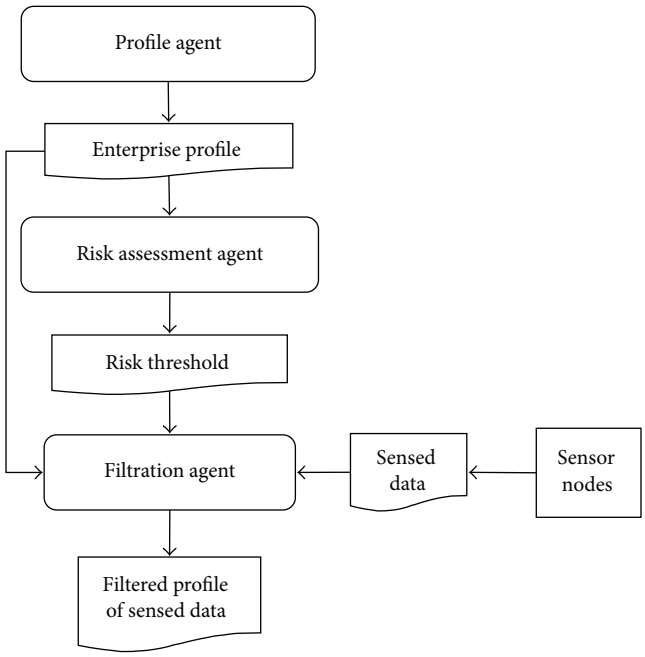

Figure 1: BPS architecture.

make adjustment to change the situation. In WSN, a lot of data is related to enterprise's sensitive information, so we have to make filtration before it is published. In the BPS, we have established a filtration agent which seeks a tradeoff between risk and utility to carry out this work. The third issue is the location privacy protection that refers to the sensors' location information in WSN. It is vital because it is related to the source and sink. In BPS, we consider this problem in the enterprise profile as the case in chapter 5 described. The fourth issue is about resisting traffic analysis. Both of DCARP and HISP-NC are good at resisting traffic analysis. We will do some work about it later to enrich our BPS. The fifth issue is about tool support. Hugin expert is used in BPS and TOSSIM is used in FRW, whereas MATLAB is used in HISP-NC. Supporting tools for DCARP have not been found.

3. Business Privacy-Protection System

In this section, we propose a business privacy-protection system (BPS) based on multiagent technology and discuss the characteristics and functions for each of the agents. Figure 1 demonstrates the BPS architecture and shows the agents and their interactions.

A Bayesian network (BN) is a directed acyclic graph (DAG), composed of representatives of the variable nodes and edges connecting these nodes. Nodes represent random variables and directed edges represent the mutual relationship between the nodes (by the parent node to its child nodes). The intensity of the relationship is expressed by the conditional probability between nodes and the no parent nodes express information with a priori probability. A BN can be used to learn causal relationships and hence can be used to gain understanding about a problem domain and to predict the consequences of intervention. Also, the BN is an ideal representation for combining prior knowledge (which often comes in causal form) and data because it has both causal and probabilistic semantics. Based on these characteristics of BN, it is suitable to predict the risk of privacy leakage.

In the BPS, there are three types of agents to be considered for simulating the process of business privacy risk protection in a WSN. These agents are described as follows:

(1) The profile agent is responsible for establishing the enterprise profile E. It includes two phases: constructing profile and customizing privacy requirement.

(2) The risk assessment agent encapsulates a BN that is employed to estimate the risk of privacy leakage. The nodes of the BN are variables that describe the risk environment for privacy leakage. The outcome of this agent is used to determine the risk threshold.

(3) The filtration agent aims to work out all possible filtered profiles to find the optimal filtration. The process of the filtration is based on two conflicting metrics named utility and risk. The outcome of this agent is a filtered profile that has highest utility and satisfies the business privacy requirement.

3.1. Profile Agent. The formal definition of enterprise profile is presented as follows.

Definition 1 (enterprise profile). The enterprise profile E is a hierarchical representation of the topic domain of an enterprise.

The enterprise profile E satisfies the assumption that, given a topic t related to the enterprise, a corresponding node can be found in E, with the subtree (t, E) as the taxonomy accompanying t. Furthermore, for each topic $t \in E$, *a profile support*, denoted by $\sup_E(t)$, represents the frequency of the topic t mentioned in E. If the topic t can be considered as the result of a random walk from its parent topic $\mathrm{Par}(t, E)$ in E, the profile support can be recursively aggregated as the following equation:

$$\sup_E(t) = \sum_{t' \in C(t,E)} \sup_E\left(t'\right), \tag{1}$$

where $C(t, E)$ is the children of t within the tree E.

The procedure of profile agent consists of the following two steps:

(1) Constructing profile.

(2) Customizing privacy requirement.

(1) Constructing Profile. The original enterprise profile E is constructed in a form of topic hierarchy as follows:

(1) Build the enterprise profile as a topic path trie with the topic set T; that is, $E = \mathrm{trie}(T)$.

(2) For topic $t \in T$, initialize the profile support $\sup_E(t)$ with (1).

Input: Set of all/candidate edges
Output: Bayesian network
//Initialization
(1) define m as the number of ants;
(2) pheromones τ: initialize each entry of τ with τ_0;
(3) define $N_{\max}$ as max number of iterations;
(4) $N_{\text{iter}} = 0$;
(5) $G^* =$ empty graph;
//Optimization
(6) **repeat**
(7) **for** $k = 1$ *to* m **do**
(8) **for** $i = 1$ to n **do** $Pa(x_i) = \phi$;
(9) **for** $i = 1$ and $j = 1$ to n **do**
(10) **if** $(i \neq j)$ **then** $\eta_{ij} = f(x_i, x_j) - f(x_i, \phi)$;
(11) **end**
(12) **repeat**
(13) Select two indexes i and j by using (5) and (6) and assign edge e_{ij} to G_k;
(14) **if** $(\eta_{ij} > 0)$ **then** $Pa(x_i) = Pa(x_i) \cup \{x_j\}$;
(15) $\eta_{ij} = -\infty$;
(16) **for all** $x_a \in$ Ancestors$(x_j) \cup \{x_j\}$ and $x_b \in$ Descendants$(x_i) \cup \{x_i\}$ **do** $\eta_{ab} = -\infty$;
(17) **for** $k = 1$ *to* n **do**
(18) **if** $(\eta_{ik} > -\infty)$ **then** $\eta_{ij} = f(x_i, Pa(x_i) \cup \{x_k\}) - f(x_i, Pa(x_i))$;
(19) **end**
(20) $\tau_{ij} = (1 - \rho) \cdot \tau_{ij} + \rho \cdot \tau_0$;
(21) **until** $\forall i, j$ $(\eta_{ij} \leq 0$ or $\eta_{ij} = -\infty)$;
(22) **end**
(23) $G_b = \arg\max_{k:1\cdots m} f(G_k : D)$;
(24) **if** $f(G_b : D) \geq f(G^* : D)$ **then** $G^* = G_b$;
(25) Update pheromone according to (3) using $f(G^* : D)$;
(26) N_{iter} + +;
(27) **until** $N_{\text{iter}} = N_{\max}$;
(28) **return** Bayesian network with structure G^*

Algorithm 1: The ACO-based algorithm for learning the BN structure.

(2) Customizing Privacy Requirement. A vulnerable node set $V \in E$ and the sensitivity sen(v) for each $v \in V$ are specified by the enterprise in this step. A vulnerable node set means that a node set belongs to the enterprise profile and may lead to privacy leakage risk to the enterprise. The *sensitivity* sen(v) represents the severity of the business privacy leakage for the enterprise due to disclosing v.

3.2. Risk Assessment Agent. This part involves risk assessment, and the risk threshold applied in profile filtration can accompany the outcome of the agent.

Ant colony optimization (ACO) algorithm [31] is an algorithm that solves the problem by simulating the embodied intelligent behavior of artificial ants groups in the process of foraging. It is a method used to find the optimal path in graph. ACO was originally used to solve TSP problem. After years of development, it has gradually penetrated other areas.

With the risk assessment agent, a BN is developed to represent the factors related to assessing the risk of business privacy leakage. To indicate the relationships among privacy risk factors, an algorithm (see Algorithm 1) based on ant colony optimization (ACO) is generated to learn the BN structure that best fits the environment of enterprise.

In each iteration, a network structure is built collaboratively by the ants on the basis of a candidate network. Each ant picks an edge at random and then decides the state of that edge based on the pheromones and heuristics in iteration. More specifically, the performances consisting of two steps of each ant are as follows.

(1) Random selection of the next edge: all edges of the graph are candidates, and the next edge will be evaluated from the set of candidates.

(2) Assignment of an edge state: this assignment is made based on probability and searches for the balance between the pheromone information and the locally computed heuristic information.

The network is changed by the ant when it finds the assignment with the highest score improvement, but the premise is that the change does not lead to any cycle in the network structure. If no higher scoring network can be found, the pheromone information is updated with the current network G and the best network found so far, G^*, to lead the ants in the next iterations to higher quality networks.

When $N_{\text{iter}} = N_{\max}$, that is, when the current number of iterations is equal to the maximum number of iterations, the

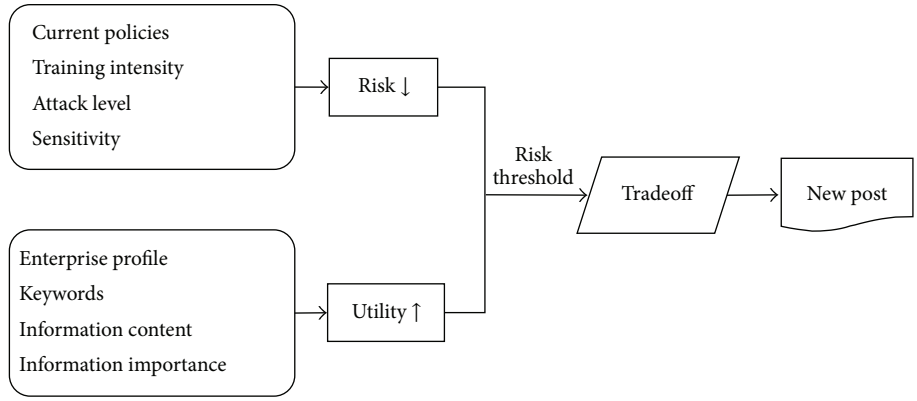

Figure 2: The filtration procedure.

process of iteration ends. $N_{\max}$ should be set to a value high enough to allow the pheromone matrix to become saturated.

The equations shown in Algorithm 1 are as follows.

(1) Heuristic Information. One has

$$\eta_{ij} = f\left(x_i, Pa\left(x_i\right) \cup \left\{x_j\right\}\right) - f\left(x_i, Pa\left(x_i\right)\right). \quad (2)$$

(2) Pheromone Updating Rule. One has

$$\tau_{ij} \longleftarrow \left(1-\rho\right)\tau_{ij} + \rho\Delta\tau_{ij}, \quad (3)$$

where

$$\Delta\tau_{ij} = \begin{cases} \dfrac{1}{\left|f\left(G^* : D\right)\right|} & \text{if } x_j \longrightarrow x_i \in G^* \\ \tau_{ij} & \text{if } x_j \longrightarrow x_i \notin G^*, \end{cases} \quad (4)$$

where τ_{ij} is the level of pheromone in the arc $x_j \to x_i$, ρ $(0 < \rho \leq 1)$ is a parameter controlling the pheromone, and G^* is the best graph found so far.

(3) Probabilistic Transition Rule. Select $x_r \to x_l$ such that

$$r, l = \begin{cases} \arg\max\limits_{i,j \in F_G} \left\{\left[\tau_{ij}\right]^{\alpha}\left[\eta_{ij}\right]^{\beta}\right\} & \text{if } q \leq q_0 \\ I, J & \text{if } q > q_0, \end{cases} \quad (5)$$

where I, J are two nodes chosen based on the following equation:

$$p_k\left(i, j\right) = \begin{cases} \dfrac{\left[\tau_{ij}\right]^{\alpha}\left[\eta_{ij}\right]^{\beta}}{\sum_{u,v \in F_G}\left[\tau_{uv}\right]^{\alpha}\left[\eta_{uv}\right]^{\beta}} & \text{if } i, j \in F_G \\ 0 & \text{otherwise.} \end{cases} \quad (6)$$

In this agent, maximum likelihood estimation (MLE) is employed to calculate the parameters (conditional probability tables) of each node in the BN based on the expert's knowledge.

After the construction of the BN of privacy leakage risk, the BN begins to act as a risk assessment tool and provides updated information about each observable node in the BN as inference evidence. The BN finally yields the occurrence probability of the risk of privacy leakage.

Table 2: The risk threshold.

Risk level	Risk threshold (β)
Very low	0.9
Low	0.7
Medium	0.5
High	0.2
Very high	0.1

To update previous estimates, the new evidence should be plugged into the BN by probabilistic inference whenever it is available in the process of the risk assessment. In BN, probabilistic inference is a task that computes all posterior marginals of nonevidence variables based on the given evidence. In this paper, an inference engine based on a junction tree is introduced.

The result of privacy risk assessment is used to determine the risk threshold, which is applied in the filtration agent. The relationship between the risk threshold and the risk level is shown in Table 2.

3.3. Filtration Agent. This agent filters the enterprise profile E in an iterative manner based on the utility and privacy risk metrics. The filtration agent is to work out all possible filtered profiles for sensed data in a WSN to find the optimal filtration. The specific procedure is as in Figure 2.

Based on the risk level estimated by risk assessment agent, the enterprise faces different levels of the privacy leakage risk. The risk may come from following four aspects.

Policy making is the first step of prevention and the enterprise must implement a policy that specifies how to manage the WSN firstly. An effective policy for WSN usage should describe permissible usage, impermissible usage, and behavioral regulations on WSN as well as access rights. In addition, the penalties for violations of the policy, including security violations and system vandalism, should also be covered. Before deploying WSN, enterprises should be required to sign a policy declaration, avowing that they

Table 3: Motivation of attacker.

Level	Definition
Weak	Out of curiosity or having no obvious motivation
Intensive	Having a strong desire to attack to benefit from valuable privacy

Table 4: Skill of attacker.

Level	Definition
Low	Collecting the public privacy on social networks
Medium	Obtaining objective privacy by text-mining or data analysis
High	Aggregating data and stealing privacy by hacking into the database of social networks

understand that it will be kept on file as a legally binding document.

Training is another proactive measure that can prevent data misuse in the company. Enterprises can effectively convey and update policies to employees by means of training, which is aimed at increasing awareness of the issues, reducing occurrence of possible incidents, and decreasing corporate liability. The components that the training focuses on are topics such as defining accessible and inaccessible data, identifying the warning signs of misuse in the workplace, and identifying risk factors that may contribute to privacy leakage. Furthermore, comprehensive employee training should cover how the company will address incidents of misuse.

The attack events are modeled with an exponential probability distribution. A successful attack on the social network is based on hackers' motivations and skills and on the vulnerability of the social network. As shown in Tables 3 and 4, the motivation range is (Weak, Intensive) and the skill range is (Low, Medium, High), both of which are obtained by expert evaluation based on the information from monitor agent.

What is more, the profile sensitivity is an important factor because different nodes have different privacy concerns. The severity of the business privacy leakage for the enterprise due to disclosure is various. Therefore, the sensitivity has a certain impact on risk. Enterprise should control the profile's sensitivity.

When confronted with the utility of the profile, the enterprise profile should be established firstly. The basic information and data about enterprise are contained. It is constructed as a tree and we can find the node in certain layer. Then we can list the keywords for every profile. The keywords help us find the current node in the tree. Based on the profile, we can also determine the information content and information importance. All these are about the utility of the profile.

Based on the risk assessment agent, we can get a risk threshold about the current situation. It is necessary to control the risk level value lower than the risk threshold. Under the premise of guaranteed risk threshold value, we establish the tradeoff to mitigate the risk and improve the utility as much as possible. Then some sensitive keywords in the profile are filtrated and the new profile is formed.

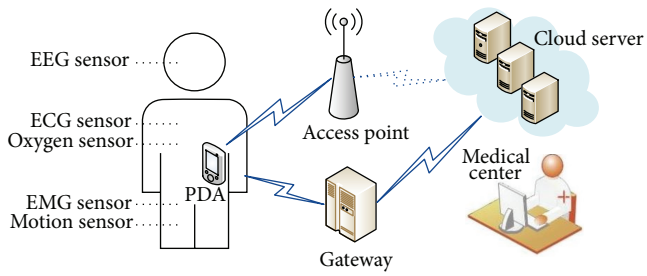

Figure 3: System architecture of medical WSN.

4. BPS Validation

Recently, the application scope of wireless sensor networks (WSNs) is wide. Many enterprises take advantage of WSN technology to expand their business [31]. In this section, the proposed BPS is applied to an Internet medical enterprise to control its privacy leakage threat.

By placing sensor nodes in the human body surface or in vivo, patients use the personal smart terminal equipment (such as PDA, smartphones) to build up WSN through self-organizing method. The network structure is shown in Figure 3. The sensors distributed in various parts of the body are used to detect physiological data (such as ECG, EEG, Pulse IPI, and Blood pressure) or peripheral status information. This collected physiological data is sent to the personal handheld devices via short-range wireless communication. Then it will be transmitted to a remote database server through the remote network. Remote medical personnel and care officers analyze the local electronic medical data to detect abnormal physiological condition of the patients and perform remote feedback treatment.

The specific workflow of the application of WSN is described as follows. By placing biological sensor nodes in patient's body, the system can detect physiological data and surrounding circumstances. Then the collected data is transmitted by wireless network to remote databases and services. After the data processing, the patients and doctors will receive the patient's current physical condition information on their personal smart terminal equipment (such as smartphone) through wireless network. Remote doctors analyze the received medical data and contact the patients in abnormal physiological conditions, and then the remote treatment and communication through the intelligent terminal are formed.

The Internet medical enterprise must attach great importance to privacy protection in WSN, because the patients' privacy disclosure will lead to very serious consequences. For example, if a patient's identification information, location information, or physical conditions are intercepted by illegal persons, it is a serious problem. Based on the patient's information, medicine marketing or some spam may be caused. Of course, these will affect people's normal life.

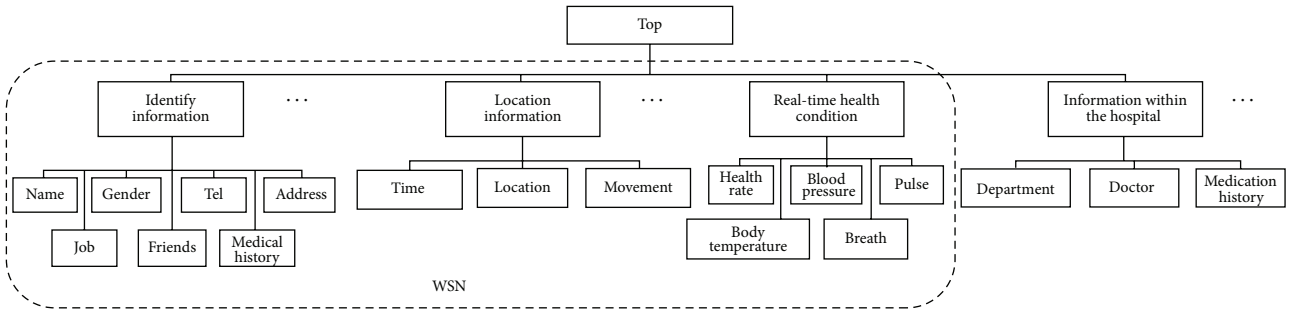

Figure 4: Sample of Internet medical enterprise profile.

Table 5: Privacy of threat node in BN.

ID	Threat node	State space	Parent nodes	Children nodes
R1	Privacy leakage threat	{High, Medium, Low}	{RF_4, RF_5, RF_6}	Ø

Table 6: Privacy of threat factor nodes in BN.

ID	Threat factor	State space	Parent nodes	Children nodes
RF_1	Skill of attackers	{High, Medium, Low}	Ø	{RF_5}
RF_2	Vulnerabilities of the WSN	{High, Medium, Low}	Ø	{RF_5}
RF_3	Motivation of attackers	{Intensive, Weak}	Ø	{RF_5}
RF_4	Enterprise security measures	{Effective, Average, Ineffective}	Ø	{RF_6, R1}
RF_5	Threat of privacy leakage through WSN	{High, Medium, Low}	{RF_1, RF_2, RF_3}	{R1}
RF_6	Awareness of privacy security	{High, Medium, Low}	{RF_4}	{R1}

A sample of the enterprise profile is illustrated in Figure 4, which is established according to the domain knowledge about the enterprise.

As shown in Figure 4, there is some information about patients in the enterprise, and here we just list a portion of distinct information that sensors in WSN can accept. When patients and doctors interact, they would generate incomplete information. For example, a patient may use vague words to describe his feelings, so that it will produce medium and ambiguous keywords. These keywords may contain sensitive information that patients do not want more people to know. Thus, every node in the tree has its own sensitivity value that represents the loss amount once privacy leakage happens.

4.1. Implementation. Based on the ACO-based algorithm presented in Section 4.2, we develop the BN encapsulated in the risk assessment agent. For the algorithm, different parameter levels are examined, following the research presented in [32]. There are six different ant colony sizes, $m \in \{5, 10, 20, 30, 40, 50\}$; four different evaporation rate levels, $\rho \in \{0, 0.25, 0.5, 0.75\}$; three different pheromone weighting parameters, $\alpha \in \{0, 1, 5\}$; and three different desirability parameters, $\beta \in \{0, 1, 5\}$. The arbitrary positive constant Q is set to 100. The initial pheromone intensity on all arcs τ_0 is fixed at 1. Meanwhile, different numbers of iterations were tested, and we found that the algorithm's performance no longer improved significantly after 500 iterations. Thus, the maximum number of iterations was set to $N_{\max} = 500$. In sum, our experiments show that $m = 30$, $\alpha = 1$, $\beta = 5$, and $\rho = 0.75$ are the best choices for the parameter values for the algorithm.

Table 7: The risk level.

Risk level	Risk state	Probability range
Very low	Low	≥0.7
Low	Low	≥0.5
Medium	Medium	≥0.5
High	High	≥0.5
Very high	High	≥0.7

Table 8: The probabilities of threat occurrence.

Threat node	State	Probability	Risk level
R1. Privacy leakage threat	High	0.6152	High
	Medium	0.2413	
	Low	0.1435	

The details of the privacy leakage risk node that security threat managers hope to predict ultimately are shown in Table 5, whereas Table 6 presents the information regarding the factor nodes of the risk node R1, that is, the causes that lead to the privacy leakage. Figure 5 shows the BN structure of privacy leakage risk and the conditional probability tables of the nodes are shown in Appendix. Moreover, the IDs of the BN nodes in Tables 9–11 and Figure 5 are explained in Tables 5 and 6.

Table 9: CPT of P (RF_5|RF_1, RF_2, and RF_3).

RF_1	RF_2	RF_3	RF_5 = high	RF_5 = medium	RF_5 = low
High	High	Intensive	0.9727	0.0273	0
Medium	High	Intensive	0.7933	0.1978	0.0089
Low	High	Intensive	0.7169	0.2653	0.0178
High	Medium	Intensive	0.7896	0.1601	0.0503
Medium	Medium	Intensive	0.7016	0.2198	0.0786
Low	Medium	Intensive	0.5607	0.3401	0.0992
High	Low	Intensive	0.6195	0.2602	0.1203
Medium	Low	Intensive	0.5538	0.3394	0.1068
Low	Low	Intensive	0.4939	0.3489	0.1572
High	High	Weak	0.7149	0.1962	0.0889
Medium	High	Weak	0.5950	0.2547	0.1503
Low	High	Weak	0.5499	0.2789	0.1703
High	Medium	Weak	0.5674	0.3011	0.1315
Medium	Medium	Weak	0.3021	0.4125	0.2854
Low	Medium	Weak	0.2201	0.3601	0.4198
High	Low	Weak	0.4650	0.3004	0.2346
Medium	Low	Weak	0.1929	0.3198	0.4873
Low	Low	Weak	0.0109	0.1688	0.8203

Table 10: CPT of P (RF_6|RF_4).

RF_4	RF_6 = high	RF_6 = medium	RF_6 = low
Effective	0.0056	0.1368	0.8576
Average	0.3028	0.5786	0.1186
Ineffective	0.8924	0.1062	0.0014

The relationship between the risk level and the probability of each risk state is shown in Table 7. We offer the updated information about each observable node in the BN as inference evidence. With regard to the privacy leakage risk, the estimated probabilities of risk state and risk level by security threat assessment are shown in Table 8. Since the privacy risk level is high, the risk threshold is set as 0.2 according to Table 2.

4.2. Experiment Results. In this section, the experimental results of BPS are presented. In this experiment, we analyze and compare the results of utility and privacy risk in the iterative process of the filtration.

Figures 6 and 7 demonstrate the results of the utility and risk during the filtration, respectively. In order to show the trend of the results clearly, we link the results on each iteration with dotted line.

In Figure 6, the graph means that, with the number of iterations increasing, the amounts of utility are gradually decreased. We can observe that the utility displays an incremental decrease during filtration. This means that the higher level topics improve the sensed information strength more effectively. Figure 7 shows the results of the metric of risk during the filtration. We observe that the privacy risk first decreases incrementally, but the decline becomes slow as more vulnerable node is pruned from the profile of sensed data.

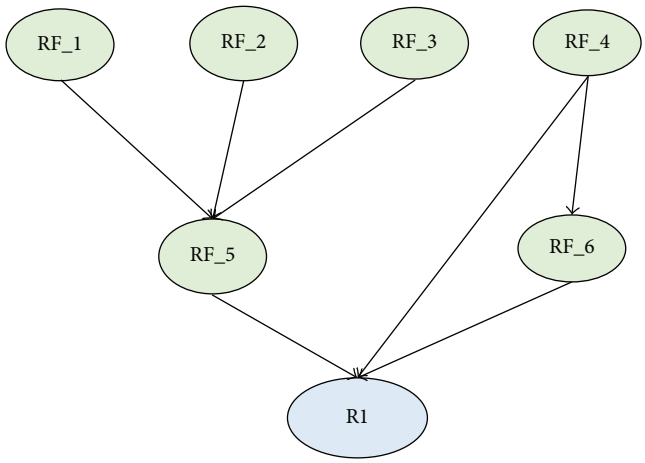

Figure 5: BN structure of privacy leakage risk.

Figure 8 illustrates the tradeoff between the utility (i.e., *IS*) and the privacy risk. For the keywords issued to the WSN, we can find that the utility increases incrementally with slight compromise on risk, while, after a turning point, any small utility will be improved at the cost of a great increase in privacy risk. Therefore, the turning point is a near-optimal solution for the tradeoff.

5. Conclusions

This paper proposes a business privacy-protection system called BPS to mitigate the threat of enterprise's privacy leakage in the application of wireless sensor networks (WSNs). The main contributions are summarized as follows.

(1) In the BPS, we develop a filtration to filter sensitive information from sensed data transmitted in a WSN

Table 11: CPT of P (R_1|RF_4, RF_5, and RF_6).

RF_4	RF_5	RF_6	R1 = high	R1 = medium	R1 = low
Effective	High	High	0.4253	0.2732	0.3015
Average	High	High	0.5435	0.2432	0.2142
Ineffective	High	High	0.6012	0.2441	0.1547
Effective	Medium	High	0.3186	0.2816	0.3998
Average	Medium	High	0.3972	0.2984	0.3044
Ineffective	Medium	High	0.5048	0.2699	0.2253
Effective	Low	High	0.0147	0.1002	0.8851
Average	Low	High	0.1738	0.3017	0.5245
Ineffective	Low	High	0.4244	0.2874	0.2882
Effective	High	Medium	0.4987	0.2671	0.2432
Average	High	Medium	0.5548	0.2883	0.1569
Ineffective	High	Medium	0.6943	0.2089	0.0968
Effective	Medium	Medium	0.4007	0.3012	0.2981
Average	Medium	Medium	0.5142	0.2844	0.2014
Ineffective	Medium	Medium	0.7045	0.1808	0.1147
Effective	Low	Medium	0.2918	0.3067	0.4015
Average	Low	Medium	0.4312	0.2555	0.3133
Ineffective	Low	Medium	0.5413	0.2498	0.2089
Effective	High	Low	0.6872	0.1883	0.1245
Average	High	Low	0.8325	0.1186	0.0489
Ineffective	High	Low	0.9701	0.0299	0
Effective	Medium	Low	0.6303	0.1972	0.1725
Average	Medium	Low	0.7152	0.1800	0.1048
Ineffective	Medium	Low	0.8047	0.1628	0.0325
Effective	Low	Low	0.5217	0.2128	0.2655
Average	Low	Low	0.6045	0.2413	0.1542
Ineffective	Low	Low	0.7012	0.2001	0.0987

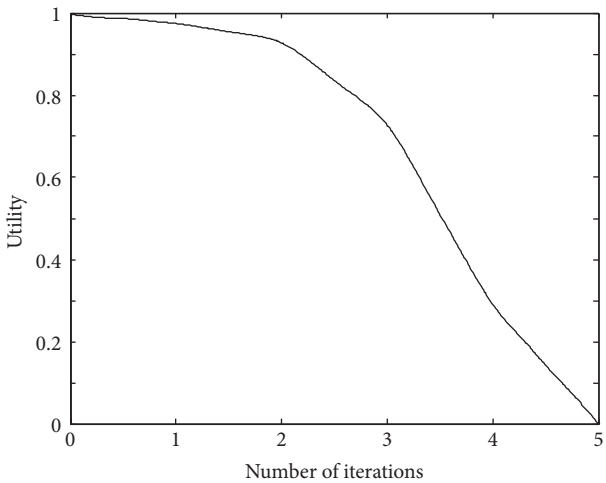

Figure 6: Results of utility.

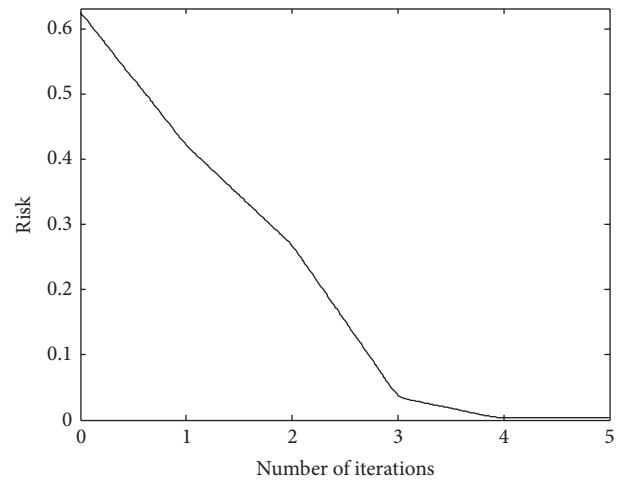

Figure 7: Results of privacy risk.

with respect to enterprise-specified privacy requirements.

(2) We formulate a tradeoff between two conflicting metrics named *utility* and *risk* in the process of profile filtration. The former one is defined as the information strength of the filtered profile of sensed data, while the latter one represents the risk of the profile exposure.

(3) We design three agents, profile agent, risk assessment agent, and filtration agent, which are interrelated and

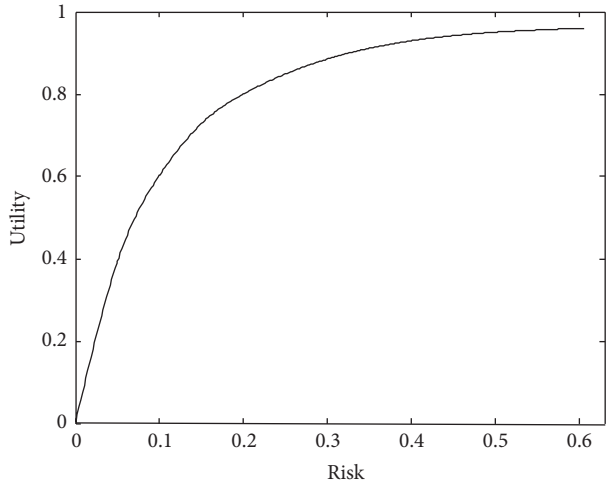

Figure 8: Utility versus risk.

interact with each other to implement the BPS based on multiagent technology.

In future work, we will focus on the automatic retrieval of the profile of sensed data based on the enterprise profile. In addition, we also try to improve the current metrics to test the performance of our proposed BPS.

Appendix

The conditional probability tables of the nodes (i.e., RF_5, RF_6, and R1) in Figure 5 are shown in Tables 9–11.

Competing Interests

The authors declare that there are no competing interests.

Acknowledgments

The research was supported by the National Natural Science Foundation of China (no. 71271149) and the Program for New Century Excellent Talents in University.

References

[1] F. Yu, C.-C. Chang, J. Shu, I. Ahmad, J. Zhang, and J. M. de Fuentes, "Recent advances in security and privacy for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 169305, 2 pages, 2015.

[2] Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of security technologies on wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 842392, 9 pages, 2015.

[3] L. Ding, F. Yu, Z. Yang, and G. Yue, "The system design of a node of p2p networks for intrusion detection," *Journal of Networks*, vol. 8, no. 8, pp. 1920–1927, 2013.

[4] A. Ramos and R. H. Filho, "Sensor data security level estimation scheme for wireless sensor networks," *Sensors*, vol. 15, no. 1, pp. 2104–2136, 2015.

[5] M. Shariati, F. Bahmani, and F. Shams, "Enterprise information security, a review of architectures and frameworks from interoperability perspective," *Procedia Computer Science*, vol. 3, pp. 537–543, 2011.

[6] D. He, C. Chen, S. C. Chan, J. Bu, and L. T. Yang, "Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 11, pp. 5348–5354, 2013.

[7] H. Huang, T. Gong, P. Chen, G. Qiu, and R. Wang, "Secure two-party distance computation protocols with a semihonest third party and randomization for privacy protection in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 475150, 15 pages, 2015.

[8] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Toward a statistical framework for source anonymity in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 248–260, 2013.

[9] R. Rios and J. Lopez, "Exploiting context-awareness to enhance source-location privacy in wireless sensor networks," *Computer Journal*, vol. 54, no. 10, pp. 1603–1615, 2011.

[10] R. Rios, J. Cuellar, and J. Lopez, "Probabilistic receiver-location privacy protection in wireless sensor networks," *Information Sciences*, vol. 321, Article ID 11369, pp. 205–223, 2015.

[11] J. D. Zhang and C. Y. Chow, "REAL: a reciprocal protocol for location privacy in wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 458–471, 2015.

[12] L. Zhang, H. Zhang, M. Conti, R. Di Pietro, S. Jajodia, and L. V. Mancini, "Preserving privacy against external and internal threats in WSN data aggregation," *Telecommunication Systems*, vol. 52, no. 4, pp. 2163–2176, 2013.

[13] R. D. Pietro and A. Viejo, "Location privacy and resilience in wireless sensor networks querying," *Computer Communications*, vol. 34, no. 3, pp. 515–523, 2011.

[14] K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: a survey," *IEEE Transactions on Systems, Man and Cybernetics C: Applications and Reviews*, vol. 42, no. 6, pp. 1243–1256, 2012.

[15] N. Zhang and W. Zhao, "Privacy-preserving data mining systems," *Computer*, vol. 40, no. 4, pp. 52–58, 2007.

[16] N. Zhang, S. Wang, and W. Zhao, "A new scheme on privacy preserving association rule mining," in *Knowledge Discovery in Databases: PKDD 2004: 8th European Conference on Principles and Practice of Knowledge Discovery in Databases, Pisa, Italy, September 20–24, 2004. Proceedings*, vol. 3202 of *Lecture Notes in Computer Science*, pp. 484–495, Springer, Berlin, Germany, 2004.

[17] N. Zhang, S. Wang, and W. Zhao, "A new scheme on privacy-preserving classification," in *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '05)*, pp. 374–383, Chicago, Ill, USA, August 2005.

[18] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 48, no. 4, pp. 393–422, 2012.

[19] E. De Cristofaro, X. Ding, and G. Tsudik, "Privacy-preserving querying in sensor networks," in *Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN '09)*, pp. 1–6, San Francisco, Calif, USA, August 2009.

[20] L. Sweeney, "*k*-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[21] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "*L*-diversity: privacy beyond *k*-anonymity," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, article 3, Article ID 1217302, 2007.

[22] R. Di Pietro, P. Michiardi, and R. Molva, "Confidentiality and integrity for data aggregation in WSN using peer monitoring," *Security and Communication Networks*, vol. 2, no. 2, pp. 181–194, 2009.

[23] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS '06)*, IEEE, Rhodes Island, Greece, April 2006.

[24] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proceedings of 25th IEEE International Conference on Distributed Computing Systems*, pp. 599–608, IEEE Computer Society, Washington, DC, USA, June 2005.

[25] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Proceedings of the 15th IEEE International Conference on Network Protocols (ICNP '07)*, pp. 314–323, Beijing, China, October 2007.

[26] A. A. Nezhad, A. Miri, and D. Makrakis, "Location privacy and anonymity preserving routing for wireless sensor networks," *Computer Networks*, vol. 52, no. 18, pp. 3433–3452, 2008.

[27] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 36–50, 2015.

[28] A. Das and M. M. Islam, "SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 261–274, 2012.

[29] Q. Yang, H. Ma, and Y. Yu, "Multi-agent risk identifier model of emergency management system engineering based on immunology," *Systems Engineering Procedia*, vol. 4, pp. 385–392, 2012.

[30] S. Bishop, H. Okhravi, S. Rahimi, and Y.-C. Lee, "Covert channel resistant information leakage protection using a multi-agent architecture," *IET Information Security*, vol. 4, no. 4, pp. 233–247, 2010.

[31] S. Jiang, Y. Cao, S. Iyengar et al., "CareNet: an integrated wireless sensor networking environment for remote healthcare," in *Proceedings of the 3rd International ICST Conference on Body Area Networks (BODYNETS '08)*, Tempe, Ariz, USA, March 2008.

[32] T. Liao, K. Socha, M. A. M. De Oca, T. Stutzle, and M. Dorigo, "Ant colony optimization for mixed-variable optimization problems," *IEEE Transactions on Evolutionary Computation*, vol. 18, no. 4, pp. 503–518, 2014.