Cross-Domain Fine-Grained Data Usage Control Service for Industrial Wireless Sensor Networks

IEEE Access
The journal for rapid open access publishing

Received October 11, 2015, accepted November 13, 2015, date of publication December 1, 2015, date of current version January 6, 2016.

Digital Object Identifier 10.1109/ACCESS.2015.2504541

Cross-Domain Fine-Grained Data Usage Control Service for Industrial Wireless Sensor Networks

JUN WU[1], MIANXIONG DONG[2], KAORU OTA[2], MUHAMMAD TARIQ[3], (Member, IEEE), AND LONGHUA GUO[1]

[1]School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[2]Department of Information and Electric Engineering, Muroran Institute of Technology, Muroran 050-8585, Japan
[3]Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

Corresponding author: M. Dong (mx.dong@ieee.org)

This work is partially supported by JSPS KAKENHI Grant Number 26730056, 15K15976, JSPS A3 Foresight Program, the National Natural Science Foundation of China under Grant 61401273 and Grant 61431008.

ABSTRACT In an industrial system, wireless sensor networks (WSNs) are usually adapted to industrial applications. Industrial system is a novel scenario to apply WSNs. Industrial WSNs are the base to establish a supervisory control and data acquisition system with the benefits of extending the network boundaries and enhancing the network scalability of the WSNs. The integration of industrial systems, such as smart grids and social networks, is an important trend for new network technologies. In many application scenarios of industrial systems, WSNs are controlled by different authorities. The network nodes that belong to different domains can share the sensor data by standard protocols. Moreover, in an applications, scenario that has high security requirements, the nodes of social networking WSNs could belong to different security levels; thus, these data can be controlled only by specific types of users. Therefore, the cross-domain fine-grained data usage is the core problem for this approach. To address this problem, this paper focuses on the cross-domain fine-grained data usage control mechanism of social networking WSNs in industrial systems, which includes cross-domain fine-grained access control and fuzzy clustering for sensing data for efficient analysis. In addition, dynamic service composition is proposed for data usage. The simulation results verify the feasibility and data usage effectiveness of the proposed scheme.

INDEX TERMS Usage control, cross-domain, fine-grained, wireless sensor networks (WSNs), clusters.

I. INTRODUCTION

Because a large amount of sensing data from industrial systems is stored in industrial wireless sensor networks (WSNs), data security naturally becomes an important concern. In fact, in many applications scenarios of industrial systems, data sensed by industrial WSNs are closely related to security and safety issues [1]–[3]. More specifically, the sensing data should be controlled by only authorized users of the industrial system.

Currently, industrial WSNs have attracted a large amount of attention, which allows the interconnection of smart objects, such as mobile robots and wireless sensors, by using different communication protocols and by developing a dynamic multi-modal heterogeneous network. Recently, WSNs have been applied widely in industry and have greatly improved the informatization and automation of these areas [4]. With the development of WSN technologies, the integration of WSNs and social networks is an important trend of new network technologies; this approach can establish social relationships in an autonomous way with the benefits of extending network boundaries and enhancing network scalability. In this new system, the nodes in WSNs can obtain social attributes and capabilities and become an important part of social networks. There are many advantages for using the attributes and ideas of social networking elements in the WSNs in industrial systems. This approach allows the nodes in industrial sensors to establish social relationships autonomously. More importantly, the nodes in social WSNs can act as the core nodes of social networks, which establishes a bridge between the social users and the physical world.

Also, some complex and novel network model, such as social networking, for industrial systems has been studied widely, especially with respect to smart grids. A more robust framework is proposed in [5] for exploring the diffusion of

basic smart grid technologies using a social network-based model to study demand response adoption in smart grids. In [6], a "family plan" approach was proposed that partitions users into groups and schedules the users' appliances to minimize the peak power consumption of each group in the smart grid. In addition, social networking WSNs have been studied widely. Reference [7] gave a definition and basic function model of a combination of social WSNs, and the benefits of this system have been widely discussed [8], [9]. Additionally, social networking WSNs have been studied extensively. Reference [10] focused on the problem of understanding how the information provided by members of the social networking WSN must be processed to build a reliable system on the basis of the behavior of objects. Some typical applications schemes based on social networking WSNs have also been proposed, such as context awareness and the service architecture for Body Sensor Networks (BSNs) in social networks [11], [12]. On the other hand, the real application systems of the social networking WSNs are under research. For example, under the support of the European-funded project, the "SMART Cities Search Engine" has been proposed. In this project, the sensors in the Internet of Things (IoT) in a city can be integrated with Twitter; thus, the users in social networks can interoperate the data from the underlying sensors, which can optimize the security, transportation, and other components of a smart city. This project has been tested in a real city in 2014 [13].

Although the novel networking models for industrial WSNs have many additional benefits compared with traditional WSNs in industrial systems, the openness, complexity and dynamics of social networks increase the risks. In recent industrial WSNs, almost all of the sensors and base stations belong to a single authority who can master the whole network. In this situation, we call it a single domain sensor network. However, in many applications scenarios, social networking WSNs are controlled by different authorities. Additionally, the network nodes that belong to different domains can share sensor data by standard protocols. How to realize the cross-domain security access for multi-domain WSNs is a research question that must be resolved. Moreover, in an applications scenario that has higher security requirements, all types of sensing data generated based on various nodes of social networking WSNs could have different levels of security. Thus, these data could be controlled only by given types of users. In other words, the usage rights of a given type of data for users are based solely on necessity. For example, the monitoring center in the smart grid scenario must be able to access all types of data for it to have overall control of the system. On the other hand, an operator could need to access only the sensing data that is relevant to his work. However, most of the existing proposals for security schemes for sensing data in WSNs have been proposed to perform uniform security. Therefore, fine-grained data control is a necessity.

To address the above challenges, this paper proposes a security fine-grained cross-domain data usage mechanism for WSNs. Section II presents the preliminaries of this paper. Sect. III gives the design principles. Sect. IV gives the proposed cross-domain secure authentication. Sect. V gives the fuzzy cluster data analysis scheme. The implementation system and evaluation are presented in Sect VI. Related studies are given in Sect. VII. Finally, Sect. VIII concludes this paper.

II. PRELIMINARIES

A. CROSS-DOMAIN DATA STORAGE AND ACCESS ARCHITECTURE

There are two main methods for WSNs to perform data storage and usage, which are centralized and distributed methods. For the centralized method, the data are sensed based on individual sensor nodes and return to a central node. For the distributed method, after the data are sensed by a sensor node, the sensor stores the data by itself or in some related nodes. Thus, the WSNs do not need to send the sensing data to a centralized node. In addition, the stored sensing data can be controlled by the users of the WSN. The cross-domain data storage and access architecture is shown in Fig. 1.

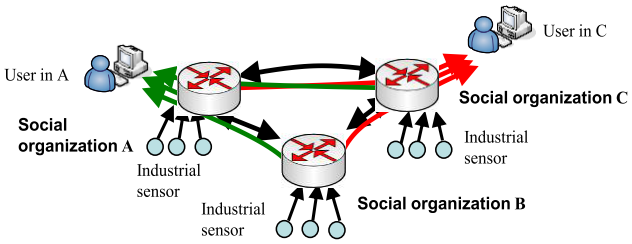


FIGURE 1. Cross-domain data storage and access.

B. BASIC TECHNOLOGIES

1) PUBLIC KEY INFRASTRUCTURE (PKI)

In cryptography, the public key infrastructure (PKI) is a system that combines public keys and given user identities through using a certificate authority (CA). In fact, PKI is a system that has a set of software, hardware, users, and policies, which can create, distribute, store, use, and revoke the digital certificates. The identity of the users should be unique in the domain of each CA. In addition, this information can be provided by the third-party validation authority (VA) on behalf of the CA. The combination process is performed through issuance and registration. The issuance depends on the assurance level of the combination and can be performed by the software of a CA. The registration authority (RA) is used to denote the role of the PKI that assures this combination. This approach can ensure that the public key corresponds to the user. PKI provides a high security level for the information system.

2) ROLE-BASED ACCESS CONTROL (RBAC)

Role-based access control (RBAC) is a useful access control method that was developed in the 1990s. The RBAC 96 method proposed by Sandhuat George Mason University became a classical role-based access control method

later. As a secure and efficient access control mechanism, RBAC was widely applied because of its introduction of the concept role, which makes it convenient to allocate and manage permissions. Users acquire corresponding permission through roles, whereby operation permission is granted to the roles rather than to the users themselves. When a user's permission changed, the user's current role takes the place of the original role. RBAC has characteristics such as a hierarchy role, minimum privilege and separation of duty. The basic RBAC method defined the most essential elements as follows: user, role, object, operation and permission, which also includes user assignment, permission assignment and session. With those elements, this method makes it possible to allocate and manage permissions efficiently.

3) USAGE CONTROL (UCON)

Usage control (UCON) is regarded as the next generation access control model. In contrast to traditional access control, it performs data control not only at the time of access but also during and after the usage [14]. Continuous decisions with regard to data usage could be performed before the usage is allowed or during the process of the usage session, with an event after the session. Additionally, the attributes can be updated before, in the process of or after the usage has been authorized. Through this type of continuous control of the data usage, the security level can be substantially improved. Some additional capabilities, such as data rights management, can be performed. In the relationship between traditional access control and usage control, the authentication process is a basic component of the usage control. The continuous access decisions are made based on the attributes and access policies. The authentication process can provide some primitive attributes that support pre-decisions. However, further ongoing decisions are based on many other dynamic attributes of subjects and objects. The definition of usage control is shown in Fig. 2.

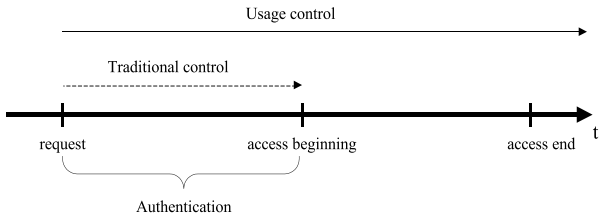


FIGURE 2. Usage control definition.

4) FUZZY CLUSTER

Cluster analysis is a type of multivariate analysis in mathematical statistics. However, because in the real world the classification always has the features of fuzzy, fuzzy clustering is the most appropriate to perform the classification and makes the classification results conform more to reality. The basic idea of fuzzy clustering is shown as follows. For a given sample set, the proper formulas are used to compute the similarity factors of different samples. Then, the fuzzy similarity relation can be achieved. Next, the similarity relations are changed to fuzzy equivalent relationships. Finally, the samples can be classified by the given rules.

III. DESIGN PRINCIPLE

A cross-domain fine-grained data usage control service is proposed to enhance the security of WSNs in industrial systems. A comprehensive set based on a data usage control Service Bus is utilized in the proposed mechanism, as shown in Fig. 3. In addition to the original Applications (APPs), Business Activity Monitoring (BAM), Rules and Tasks, security service protects the data with Service Manager and Service Composition. Security management toward DR events relies on the two security services, which include a cross-domain fine-grained data access service (CUS) and a data analysis service (DAS). Service Manager provides the centralized management of the original service and additional security services such as versioned, private and public service types in the sensor networks in the industrial systems. Service Manager includes a Service Registry and a Service Repository, which enable the versioning and reuse of service types, and a Service Dispatcher provides a publish/subscribe communication framework.

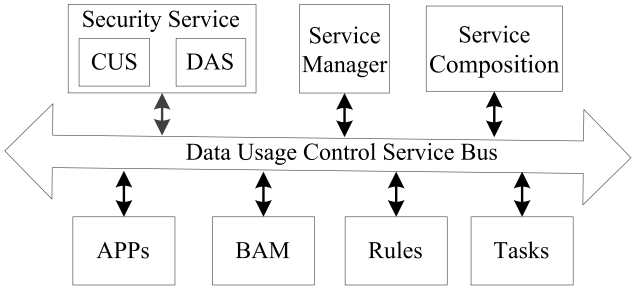


FIGURE 3. Proposed security service mechanism for WSNs data.

The three major security services are provided to protect the system that is achieved by the fine-grained sub-services under the dispatch of the service manager, service composition and service selection, as shown in Fig. 4. Considering the security and efficiency requirements of the proposed mechanism, the sensing data storage service includes data

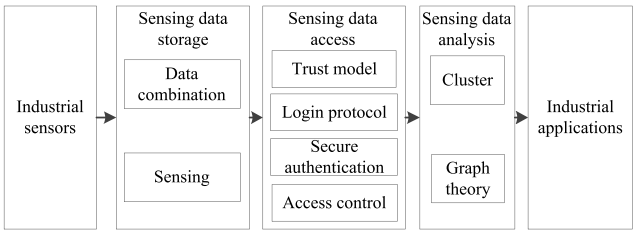


FIGURE 4. Basic idea of the proposed security service.

sensing and combination capabilities. Security access service toward the sensing side probes the security-related data from the industrial sensors. Based on the certificate assignment method of X.509 (according to ISO/IEC 9594-8), the system

integrates the characteristics of WSNs. A username/password security token is used to perform the use login protocol. An access control method is utilized to allocate permission based on the probed data. The username/password token with the help of a dynamic password provides a more secure authentication. In addition, sensing data analysis services can perform the fine-grained data analysis.

IV. CROSS-DOMAIN SECURE ACCESS SCHEME

In the application, we can regard a domain as a network that belongs to a single authority. In addition, the security requirements are relatively low. The number of users is relatively limited, and the authentication in the domain is relatively simple. Hence, symmetric key cryptography (SKC) is sufficient for the secure authentication of single-domain WSNs, as in our previous work. However, secure authentication for a cross-domain is very complex, and public key cryptography (PKC) combined with SKC is needed to resolve the question. The notation used in this section is shown in Table 1.

TABLE 1. Notations used in the proposed scheme.

A. TRUST MODEL FOR CERTIFICATE AUTHORITY (CA)

Based on the certificate assignment method of X.509 (according to ISO/IEC 9594-8), integrating with the characteristics of WSNs, we propose the trust model for authority in industrial WSNs.

The framework is a multilayer tree structure in a domain. Moreover, it is a mesh structure among the domains. Each greyer certificate authority (CA) is a root CA because a trust anchors in a domain. For the WSNs that have distributed data storage, we use a two-layer tree structure, such as Domain1. The top layer CA_1 is designed in the base station to be the root CA and can issue data certificates and distribute keys to the second-layer CA, such as CA_{11}. In addition, the CAs at the second layer are designed in the nodes in which the sensed data are stored. These CAs can issue data certificates and distributed keys to the data servers and users. In our scheme, the data server is also in the nodes in which the data are stored.

For the WSNs with centralized data storage, we use only a single-layer structure, such as Domain 2. In the root CA, CA_2 is designed into the base station or the single sink. CA_2 can issue data certificates and distributed keys to the data servers and users. In addition, the server is in the node in which the data are stored, which is the base station or sink.

B. LOGIN PROTOCOL FOR THE USER

Next, we define some notation that is used in the secure authentication and key distribution protocol.

In our scheme, the user login to the WSN is based on a password. The user will log into the WSN when she needs to access the data. Then, the user will begin the login protocol. The login protocol is described as follows:

Step 1: $U \rightarrow AS : \{ID_U, P, RN_1\}_{PK_{AS}}$

When user U logs into a domain of the WSN, she generates a random value RN_1 and then encrypts P, ID_U and RN_1. Next, the user sends the ciphertext to the access server (AS), such as the base station or sink or sensor, which stores the data.

Step 2: $AS \rightarrow U : \{RN_2, ID_U\}_{RN_1}$

After AS receives the request message from U, she decrypts the message by her private key SK_{AS}; then, she obtains the ID_U and P and authenticates the identity of U. After the identity authentication, AS generates a random value RN_2; then, she encrypts RN_2 and ID_U by the symmetric key RN_1; next, she sends the ciphertext to U.

Step 3: After U receives the ciphertext from AS and subsequently decrypts the ciphertext by RN_1, she then obtains the RN_2 as the session key for the access from U to AS.

C. CROSS-DOMAIN SECURE AUTHENTICATION PROTOCOL

Step 1:

$U \rightarrow AS_h : ID_U, \{ID_S, N_U, T_U, R_U, h(T_U, R_U)\}_{K_{U,AS}}$

U sends an access request to the AS_h in her domain to ask access to the server S in another domain. N_U in the access request is the random value generated by U to ensure that the request is fresh. T_U and R_U are the additional elements to resist against the reply attack.

Step 2: $AS_h \rightarrow AS_v : ID_{AS_h}, S_{hv}$

AS_h decrypts the message from U and then checks which domain AS_h belongs to by ID_S. Then, AS_h generates the random value N_{hv} and computes $S_{hv} = \alpha^{N_{hv}} \bmod P$.

Step 3: $AS_v \rightarrow AS_h : S_{vh}, \left\{Cert.AS_v, \{h(S_{vh}, S_{hv})\}_{SK_v}\right\}_{K_{vh}}$

AS_h generates a random N_{vh} and, then, computes $S_{vh} = \alpha^{N_{vh}} \bmod P$ (according to the Diffie-Hellman key exchange scheme, which is $K_{vh} = K_{hv} = S_{vh}^{N_{hv}} \bmod P = S_{hv}^{N_{vh}} \bmod P$).

Here, K_{vh} acts as the temporary session key between AS_v and AS_h. AS_v decrypts her public key certificate chain and the digital signature of $h(S_{vh}, S_{hv})$ by K_{vh}. Then, AS_v sends the ciphertext and S_{vh} to AS_h.

Step 4:

$$AS_h \rightarrow AS_v : \left\{ \begin{array}{l} Cert.AS_h, \{h(S_{hv}, S_{vh})\}_{SK_h}, ID_U, ID_S, \\ sk, T_U, R_U, h(T_U, R_U), \{ID_U, sk\}_{N_U} \end{array} \right\}_{K_{hv}}$$

After AS_h receives the message from AS_v, AS_h computes K_{hv} and K_{vh} based on the method of Step 3 according to S_{vh}. Thus, AS_h obtains the certificate chain of AS_v and the digital signature to verify the identity. After verification, AS_h sends AS_v a message that is encrypted by K_{hv}. The message includes the certificate chain of AS_h, the digital signature, identity information of U and S, the random value sk as the session key between U and S, and the ticket $\{ID_U, sk\}_{N_U}$.

When an AS verifies the intra-domain certificate chain of another access server, she looks for the CA that can be trusted and can implement cross-authentication with the root CA of the intra-domain certificate chain. Then, a trust chain can be established, and AS can use the public key of the root CA of the intra-domain to verify the certificate chain.

Step 5:

$AS_v \rightarrow S : \left\{ID_U, ID_S, sk, T_U, R_U, \{ID_U, sk\}_{N_U}, N_v\right\}_{K_{S,AS}}$

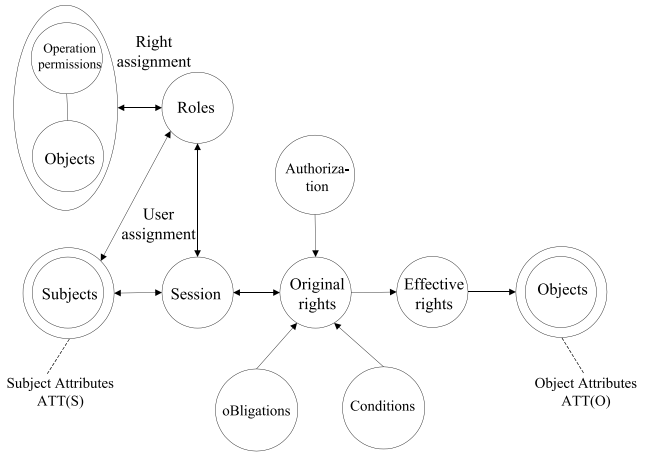


FIGURE 5. Role-based usage control for access.

AS_v verifies the identity of AS_h based on the method in Step 4 and then sends S the identity of U and S, sk, ticket $\{ID_U, sk\}_{N_U}$ and the random value for fresh. All of the data are encrypted by $K_{S,AS}$.

Step 6:

$S \rightarrow U : \{ID_U, sk\}_{N_U}, \quad \{ID_S, T_S, R_S, h(T_S, R_S), N_S\}_{sk}$

After S receives the message from AS_V, she decrypts the message by $K_{S,AS}$. Then, she sends the ticket $\{ID_U, sk\}_{N_U}$ to U; at the same time, she encrypts her information by sk and then sends it to U.

Step 7: $U \rightarrow S : N_S + 1$

After receiving the message from S, U decrypts $\{ID_U, sk\}_{N_U}$ by N_U. Then, U obtains the address of S through decrypting the information of S by sk, and afterward, U sends $SN_S + 1$ as a response and verifies her identity to S. Last, U accesses the data in S through the session key $K_{U,S}$.

D. CROSS-DOMAIN FINE-GRAINED ACCESS CONTROL

In our previous work [2], we presented the importance and possibility of designing a usage control-based access scheme for WSNs. In fact, the usage control is regarded as the next generation access control abstract framework. Because RBAC is simple for applications and flexible for extension, it is promising that we realize usage control based on RBAC.

In the model, there are 5 control functions as follows: user assignment, right assignment, authorization, obligations and conditions. User assignment and right assignment are right giving functions, and the other three functions are for right removing.

We use a hierarchy role model for the cross-domain role mapping. The model is based on inherited relations, which means that the parent roles have all of the rights of the child roles. The cross-domain role mapping is shown in Fig. 5. The role "Vice administrator" in domain B is mapped to the role "Advanced user" in domain B. This arrangement means that if a user in domain B is assigned the role "Vice administrator", she will have the rights of the role "Advanced user" in domain A when she implements cross-domain access

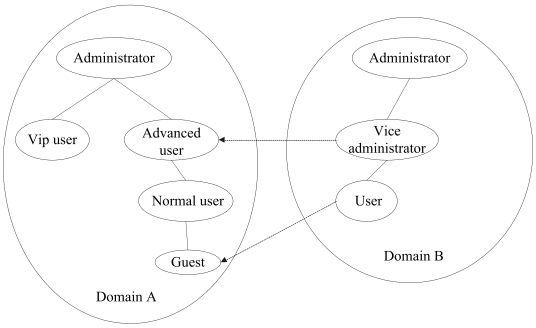


FIGURE 6. Cross-domain role mapping.

to domain A. Moreover, role mapping can be transferred. For example, in Fig. 6, when "Vice administrator" is mapped to "Advanced user" according to the hierarchy structure of role, all of the parent roles of "Vice administrator" in domain B are mapped to "Advanced user" in domain A.

V. SENSING DATA CLUSTERING ANALYSIS

With the development of the breadth and depth of monitoring for the industrial system, it is very important to propose an efficient method for analyzing the industrial sensing data. Cluster analysis is a type of multivariate analysis in mathematical statistics. However, because in the real world, the classification always has the feature of fuzzy, fuzzy clustering is more appropriate when performing the classification, and it makes the classification results conform more to reality. We use graph theory to realize the data cluster [15], [16].

A. FUZZY EQUIVALENT RELATION

In classical mathematics, an equivalent relation is usually used to classify the objects. Fuzzy cluster analysis is also based on fuzzy equivalent relations.

Definition 1: Assume that X, Y are two nonempty sets and the fuzzy subset of the following product sets is a fuzzy relation between X and Y.

$$X \times Y = \{(x, y) | x \in X, y \in Y\}$$

The membership function of is $\tilde{F}$.

$$\mu_{\tilde{F}} : X \times Y \rightarrow [0, 1]$$

For a given ordered pair $(x, y) \in X \times Y$, $\mu_{\tilde{F}}$ is the $\tilde{F}$ degree of correlation of x and y, specifically when $X = Y$, $\tilde{F}$ is called the fuzzy relation on X.

Definition 2: Assume that X, Y, Z are three nonempty sets, and $\tilde{F}_1$ is the fuzzy relation between X and Y, $\tilde{F}_2$ is the fuzzy relation between Y and Z, and $\tilde{F}$ is the fuzzy relation between X and Z. For arbitrary $(x, y) \in X \times Y$, the following formula exists:

$$\tilde{F} = \bigvee_{y \in Y} [\tilde{F}_1(x, y) \wedge \tilde{F}_2(y, z)]$$

where $\tilde{F}$ is a compositive relation between $\tilde{F}_1$ and $\tilde{F}_2$.

When X, Y, and Z are denoted as $X = \{x_1, x_2, \cdots, x_m\}$, and $Y = \{y_1, y_2, \cdots, y_l\}$, $Z = \{z_1, z_2, \cdots, z_n\}$, $\tilde{F}_1 =$

(f_{ij}) $\tilde{F}_2 = (f_{jk})$, and $\tilde{F}_3 = (f_{ik})$ are an $m \times l$, $l \times n$, $l \times n$ order fuzzy matrix. The following formula can be used:

$$f_{ik} = \bigvee_{i=1}^{l}(f_{ij} \wedge f_{jk}), \quad (i = 1, 2, \cdots, l; k = 1, 2, \cdots, n)$$

More specifically, assume that $\tilde{F}$ is the fuzzy relation on X, and $\tilde{F}^2 = \tilde{F} \circ \tilde{F}$, and $\tilde{F}^2$ is still the fuzzy relation on X. Then, for arbitrary $(x, z) = X \times X$, the following formula can be obtained:

$$\tilde{F}^2(x, z) = \bigvee_{y \in X}[\tilde{F}(x, y) \wedge \tilde{F}(y, z)]$$

Similarly, $\tilde{F}^n$ can be defined.

Definition 3: Assume that $\tilde{F}$ is the fuzzy relation on X. If x and y are selected randomly and $x, y \in X$, then $\tilde{F}$ is satisfied by the following items.

1) Reflexivity: $\tilde{F}(x, x) = 1$
2) Symmetry: $\tilde{F}(x, y) = \tilde{F}(y, x)$
3) Transitivity: $\tilde{F}^2(x, y) \leq \tilde{F}(y, x)$

Here, $\tilde{F}$ is the fuzzy relation on X, and if $\tilde{F}$ satisfies only reflexivity and symmetry, then $\tilde{F}$ is called the fuzzy relation on X. The corresponding matrixes are called the fuzzy equivalent matrix and fuzzy similar matrix, respectively.

The corresponding features between fuzzy equivalent relations and normal relations are very useful for the applications of fuzzy clustering. On the domain of discourse D, the equivalent classes coursed by general equivalent relations are a type of partition of D. In other words, the domain of discourse D can be divided into a number of non-intersecting subsets based on the equivalent relations. Thus, any element of D must belong to one of the subsets. This type of partition for D, based on equivalent relations, is a clustering. However, for fuzzy equivalent relations, the situation is more complex. The reason is that for an arbitrary two elements u and v, we cannot use the owner-member relationship to describe the relation between (u, v) and $\tilde{F}$. Membership degree can be used to describe this situation. In other words, u and v have the relation to some degree, and thus, the bound of λ is fuzzy, and the elements of D cannot be classified based on only $\tilde{F}$. If $\tilde{F}_\lambda$ is the fuzzy equivalent relation, then for arbitrary $\lambda \in [0, 1]$, it is a normal equivalent relation. In addition, D can be partitioned based on $\tilde{F}_\lambda$, and thus, a value of $\tilde{F}_\lambda$ can be obtained for a given value of λ. Different λ will generate different, and the partitions of D are different. Therefore, fuzzy equivalent relations can realize the partitions of D based on the value of $\tilde{F}_\lambda$.

B. FUZZY CLUSTER ANALYSIS

The basic idea of clustering is using a scale of similarity to measure the closeness degree, based on which classification can be realized. The essence of fuzzy cluster analysis is the construction of fuzzy equivalent relations based on the attributes of the objects, which can perform classification for the samples.

The process of clustering based on fuzzy relations is shown as follows.

Step1: Assume the sample set $X = \{x_1, x_2, \cdots, x_n\}$, where $x = \{x_{i1}, x_{i2}, \cdots, x_{im}\}$, (i = 1, 2, . . . , n). The original data of all of the indicators of xi should be standardized. Then, appropriate formula should be used to compute the similarity factor among all of the x_i and x_j, and the fuzzy relation matrix $\tilde{F} = (f_{ij})_{n \times n}$ should be established. Generally speaking, $\tilde{F}$ is obtained based on the above rules and is a fuzzy similar relation.

Step 2: The transitive closure of $\tilde{F}$ is denoted as $t(\tilde{F})$ and should be obtained, which is the fuzzy equivalent relation of $\tilde{F}$.

Step 3: According to the requirements of the real question, an appropriate $\lambda \in [0, 1]$ should be chosen. Then, the λ partition set of $t(\tilde{F})$, which is denoted as $t(\tilde{F})_\lambda$, should be computed. Then, a classification result of X can be obtained.

C. MAXIMUM SPANNING TREE FOR FUZZY CLUSTERING

It is necessary to use transitive closure to realize cluster analysis based on fuzzy equivalent relations. Here, we use the maximum spanning tree to realize fuzzy clustering for industrial sensing data.

Assume the sample set $X = \{x_1, x_2, \cdots, x_n\}$; the fuzzy similar matrix according to all of the indicators of x_i is $\tilde{F}$. This type of cluster problem can be denoted as $\langle X, \tilde{F}\rangle$. An empowerment complete graph corresponds to it, which can be called a fuzzy relation graph $G(X, E, \tilde{F})$, in which the edge $x_i x_j$ empowers. Thus, the X clustering is the vertex set of the vertex set of subdivision G.

Definition 4: Assume that T is a spanning tree empowerment connected graph. If the following formula is workable for any spanning tree of G, then T is the maximum spanning tree of G.

$$\sum_{e \in E(T')} w(e') \leq \sum_{e \in E(T)} w(e)$$

Definition 5: In the fuzzy relation graph $G(X, E, \tilde{F})$,

(1) The minimum value of the edge weights on path L is called the connection strength, which is denoted as $S(L)$ and is computed as follows.

$$S(L) = \bigwedge_{e \in E(L)} w(e)$$

where $E(L)$ denotes the edge set of path L.

(2) The maximum connection strength of all of the paths between the two points u and v is called the connection strength between u and v, which can be denoted as $S(u, v)$ and is computed as follows.

$$S(u, v) = \bigvee_{i=1}^{k} S(L_i), \quad (u \neq v)$$

where $S(u, u) = 1$

(3) Assume that L is the path that connects u and v in G. If $S(L) = S(u, v)$, then L is the optical path that connects u and v in G.

In addition, assume that T is a spanning tree of the fuzzy relations graph $G(X, E, \tilde{F})$; then, the following descriptions will be workable.

(1) T is the maximum spanning tree of G.
(2) For arbitrary $e' \in E(T)$, T_1 and T_2 can be obtained through moving e' from T, and the following formula is workable.

$$w(e') = \underset{e \in [T_1, T_2]_G}{\vee} w(e)$$

(3) For arbitrary $u, v \in X (u \neq v)$, then the only path between u and v in T is the optimal (u, v) path in G.

In addition, if $X = \{x_1, x_2, \cdots, x_n\}$, and the fuzzy similar relation on X is denoted as $\tilde{F} = (f_{ij})_{n \times n}$, then the transitive closure of the fuzzy relation $\tilde{F}$ is $t(\tilde{F}) = \tilde{F}^n = (f_{ij}^n)_{n \times n}$, the corresponding fuzzy relation graph of $\langle X, \tilde{F} \rangle$ is $G = (X, E, \tilde{F})$, and the following formula is workable:

$$t(\tilde{F})(x_i, x_j) = f_{ij}^{(n)} = S(x_i, x_j)$$

Here, x_i and x_j can be classified into a class on λ, which is equivalent to having a path whose strength is no less than between vertex x_i and x_j in the fuzzy relations graph $G(X, E, \tilde{F})$. Therefore, the cluster can be performed on G directly. The method is to find a path whose strength is no less than; then, x_i and x_j belong to the same class on the level of λ.

However, it is difficult to find a path whose strength is no less than λ between two vertexes in the fuzzy relations graph G. However, if a graph can be constructed in which there is only one path L that connects two arbitrary vertexes x_i and x_j and makes $S(L) = \mathrm{S}(x_i, x_j)$, then it is convenient to perform clustering based on λ.

In the maximum spanning tree T in a fuzzy relations graph G, the strength of the only path L between u and v is $S(L) = S(u, v)$. Thus, it is a key issue to find the maximum spanning tree T in a fuzzy relations graph $G = (X, E, \tilde{F})$. If T has been obtained, for arbitrary λ, the disconnected subgraph can be obtained whose connected branches are the classes of X on λ. The Kruskal circle method can be used to obtain the maximum spanning tree solely based on the fuzzy similar matrix directly without a fuzzy relations graph. The algorithm is shown as follows.

Assume a fuzzy similar matrix and that the level of the cluster is λ; let B_k denote the sink node set and $f_{ij} = f(x_i, x_j)$.

The following is the algorithm:

(1) Select a vertex $v_1 \in X$, which is denoted as $B_1 \in \{v_1\}$.
(2) Assume that $v^* \in C_1 = X \backslash B_1$, which makes $f(v^*, v) = \underset{v \in C_1}{\vee} = (v, v_1)$. Then, if v^* is denoted as v_2, the following formulas are workable.
(3) Assume that k vertexes are removed ($k < n$). In other words, if $B_k = \{v_1, v_2, \cdots, v_k\}$ and the $(k-1)$ edges of the graph is $E_{k-1} = \{e_1, e_2, \cdots, e_{k-1}\}$, and $v^* \in C_k = X \backslash B_k$ make $f(u^*, v^*) = \underset{u \in B_k, v \in C_k}{\vee} f(u, v)$; then, v^* is denoted as v_{k+1}, and the following formulas are workable.

$$e_k = \left(u^*, v_{k+1}\right) \left(u^* \in B_k\right)$$

$$B_{k+1} = B_k \cup \{v_{k+1}\}$$
$$E_k = E_{k-1} \cup \{e_k\}$$

(4) Given that $k = n - 1$ and the maximum spanning tree is T. When, all of the connected branches of T after removing all of the edges e is a class of X on λ. Then, the algorithm is finished; otherwise, set $k = k + 1$ and return (3).

D. OPTIMIZING FUZZY CLUSTERING

The comparison times of the above fuzzy clustering algorithm are as follows:

$$\sum_{k=1}^{n-1} [k\,(n-k) - 1] = \frac{1}{6} n^3 + O\left(n^2\right)$$

Therefore, the complexity is $O(n^3)$.

To reduce the complexity of the algorithm, Dijkstra's algorithm can be used to follow the method in graph theory of the valuation of the minimum spanning tree of the empowerment connected graph. Then, the algorithm to perform the evaluation of the maximum spanning tree of the fuzzy relation graph is as follows:

(1) Select arbitrarily a vertex $v_1 \in X$, and let $B_1 = (v_1)$, $l(v_1) = 0$, $l(v) := f(v_1, v)$, and following formula is workable.

$$p(v) := v_1 (\forall v \in X \backslash A), \quad k := 1$$

(2) Compute $\max\limits_{v \in X \backslash A_k} l(v) = l(v^*)$, and let $B_{k+1} = B_k \cup \{v^*\}$, for every $v \in X \backslash A_{k+1}$, if $r(v*) > l(v)$, $l(v) := f(v^*, v)$, $p(v) := v^*$.
(3) If $k = n-1$, according to the pointer $p(\cdot)$, the maximum spanning tree T can be traced contraorbitally. Given $k = n - 1$ and the maximum spanning tree T. When $w(e) < \lambda$, all of the connected branches of T after removing all of the edges e is a class of X on λ, and the algorithm is finished; otherwise, let $k = k + 1$ and return to step (2).

Here, steps (1) and (2) confirm the first vertex and must be performed $2(n-k) - 1$ times in comparison. Therefore, the times of the comparisons should be performed as

$$(n-2) + \sum_{k=2}^{n-1} [2\,(n-k) - 1] = (n-2)\,(n-1)$$

Therefore, the complexity of the algorithm is $O(n^2)$.

In fact, the empowerment maximum spanning tree of the connected graph has non-uniqueness, but this arrangement has no impact on the connected strength between x_i and x_j. In other words, the fuzzy cluster method for the maximum spanning tree does not depend on the selection of the maximum spanning tree.

VI. IMPLEMENTATION SYSTEM AND EVALUATIONS

A. IMPLEMENTATION SYSTEM

We use multi-agents to implement the function of UCON and chance discovery-based intrusion detection in WSNs. Figure 7 shows the architecture of the agent system of a node in an industrial WSN. The access flow and usage control system component are shown in Fig. 8.

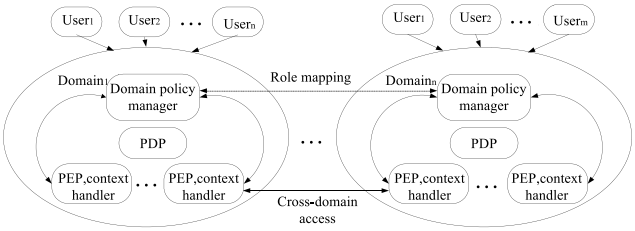


FIGURE 7. Fine-grained cross-domain usage control system.

Basically, the access control policy is to store in this component. Additionally, the policy is aggregation as a server. There are two sub-modules in the policy management module according to the functions requirement from the core RBAC model, the Element Sets management agent and the Relationship maintenance agent.

The Element Sets management agent is a domain-based module for element management. According to the definition of the National Institute of Standards and Technology (NIST), the basic elements include users, roles, objects, and operations. There are two classes of these elements, which are (1) operations and objects and (2) users and roles. When the RBAC system is applied for a resource or service, the operations and objects are relatively static. In contrast, the role set and user set are relatively dynamic. The domain policy manager is in charge of the above issues. The *AddUser* and *DeleteUser* operations for the users provide functions for the creation and deletion of the roles. the *AddRole* and *DeleteRole* operations for the roles have similar capabilities. The user and role repository can store the elements set.

The relationship maintenance agent module performs three policy assignment operations: user-to-role assignment (UA), permission-to-role assignment (PA) and cross-domain role mapping (RM). The scalable and dynamic benefits depend on the domain. This module includes the *AssignUser* and *DeassignUser* operations for UA, the *GrantPermission* and *RevokePermission* operations for PA and the AddMapping and DeleteMapping operations for RM.

The Context Handler Module is a component that can translate access requests in native format with a canonical form that is based on the standard protocol across the security domains. In addition, this module can also translate the authorization decisions into a canonical form.

The PDP (policy decision point) module is the decision center of the network and can be regarded as the policy server. The PDP stores and calls the policy in the policy manager and makes the decisions based on the decision information; then, it assigns the decisions to the corresponding PEP. PDP can

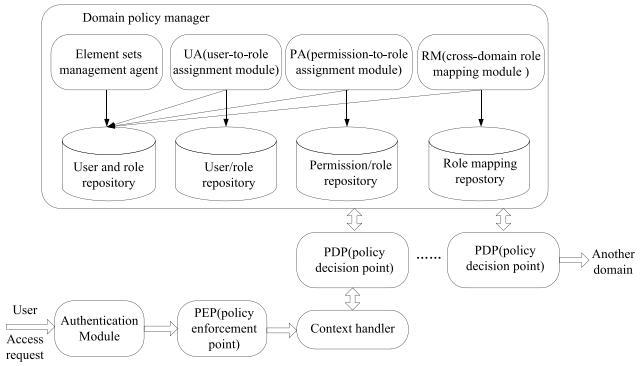


FIGURE 8. Access flow and usage control system components.

detect the change and conflict of the policies and implements the corresponding actions. PDP obtains the access request from Context Handlers and provides responses based on the police set from the domain policy administrator.

The PEP (policy enforcement point) module is the entity of the network that accepts the management of the policy and can be regarded as the policy client. The PEP can be logical or physically routed, a gateway, or other equipment of the WSN, and it can implement the policy from the PDP. In addition, the PEP can send a message to the PDP to enable the PDP to know the situation of the WSN and the implementation of the policy.

B. EVALUATIONS OF ACCESS CONTROL

In this section, we perform related simulation experiments for evaluating the feasibility and efficiency of the proposed cross-domain security access control scheme.

In the first simulation experiment, we evaluate the time overhead of the security service selection according to the increase in the number of selected services. The computer platform used in the simulation includes a 2.53 GHz Intel i5 CPU with 2GB of memory. The overhead time is shown in Fig. 4. The proposed scheme is performed in NetLogo [17] and obtains the service selection results, which are inputted into Matlab to obtain visual outputs. The number of nodes in the industrial WSNs is 200. The related security factors, including the exploitability, credibility and severity, are from the Open-Source Vulnerability Database (OSVDB) [18]. For each viewpoint in the horizontal axis, such as 20 selected security services, we perform the simulation 50 times and compute the average overhead time as the horizontal axis.

As shown in Fig. 9, with an increase in the number of nodes and as the domains increase, the overhead times also increase.

It is very important to evaluate the access control capabilities. To evaluate the control capability, the precision rate is defined as follows:

$$P_r = \begin{cases} \dfrac{SecAcc}{AllAcc}, & AllAcc > 0 \\ 0, & AllAcc = 0 \end{cases}$$

where *SecAcc* is the number of security accesses that were performed based on the proposed scheme, and *AllAcc* is

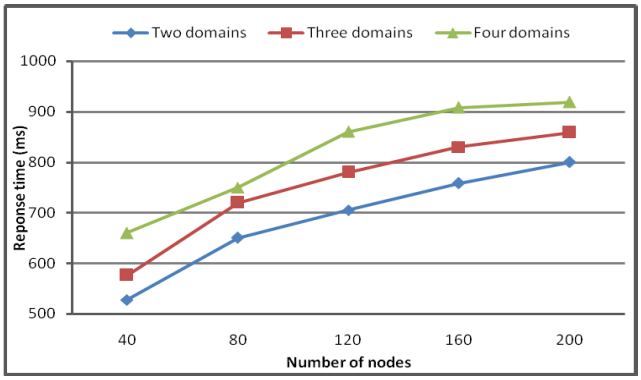


FIGURE 9. Response time of the access.

all of the accesses in the Industrial WSNs. Based on the definition, P_r is satisfied with. The value of P_r denotes the capability of the access control. The simulation results are shown in Fig. 10.

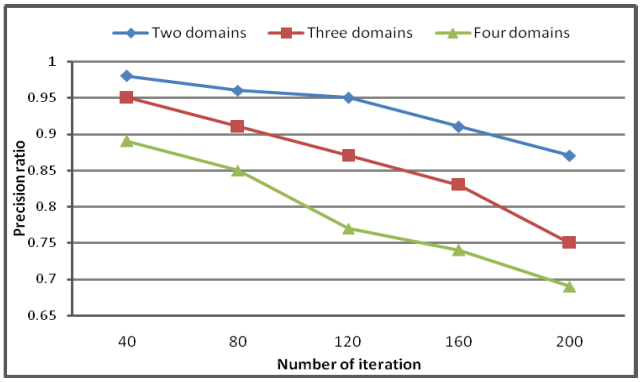


FIGURE 10. Capability of the security access control.

C. EVALUATIONS OF CLUSTER ANALYSIS

The data cluster analysis experiment is performed on cluster computers with 20 nodes, in which every server has a 2.53 GHz Intel i5 CPU and 8GB of memory. In addition, the servers are connected based on a 1G router. Hadoop-1.0.4 is used as the tool for the experiment. For comparisons, we perform the data analysis experiment at 5 nodes, 10 nodes, 15 nodes, and 20 nodes. We use python script to generate randomly the data set to simulate the sensing data in the industrial system. The sizes of the data are 1 MB, 5 MB, 10MB, and 50MB, respectively. The overhead time of the data analysis is shown in Fig. 11.

Figure 11 shows the overhead time of the data analysis when the size of the data set is changed. When the size of the data set is small, the small computer server cluster is more efficient. However, when the size of the set increases, a large server cluster is more efficient. This trend occurs because when the size of the data is small, the complexity of the computation is low, and it is faster to use fewer servers. The communications overhead is too large when large-cluster servers are used. However, when large-size data must be analyzed, the computation overhead time from using a single computer is large, and it is faster to use distributed computation.

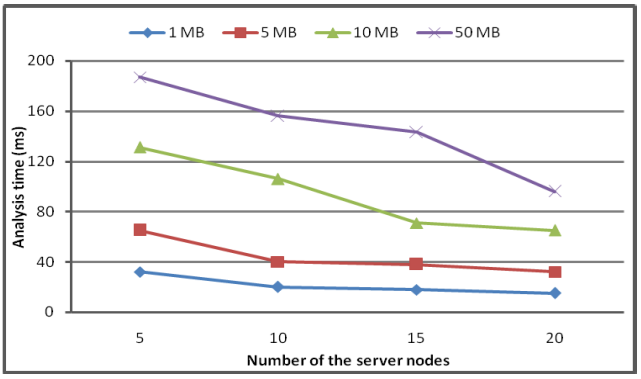


FIGURE 11. Time overhead of data analysis.

VII. RELATED STUDIES

In fact, there are many existing studies that have focused on the area of cross-domain security. The study in [19] is based on the basic idea of a cloud service consumption and delivery method, and across-domain, distributed architecture scheme was provided. Enforced traditional mandatory access control also attracted much attention, such as the Bell-LaPadula model, which is used in [20]. In a case in which different security domains had different owners, the data-sharing problem can be resolved based on this work. In addition, when the data is in a heterogeneous domain system, the work in [21] proposed a new authentication model, mainly by using PKI technology. In a Service-Oriented Architecture (SOA), the work in [22] resolved the cross-domain authentication problem, which used the service bus. Attribute-Based Access Control (ABAC) is used in [23] to perform cross-domain access control. In the work in [24], the authors considered that designing a universal model could better satisfy the special security requirements of military applications. Some existing studies focus on the data usage of industrial systems [25], [26].

Although the above existing research proposed some cross-domain security schemes for different systems, the features of complexity, randomness and dynamics of industrial WSNs were not considered. In addition, an efficient mechanism that includes cross-domain fine-grained data access control and analysis is necessary. The results in the present paper resolve this problem.

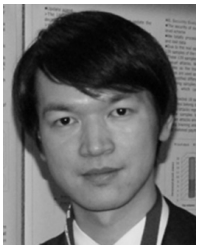
VIII. CONCLUSIONS

The openness, complexity and dynamics of WSNs increase the risks of in industrial systems. Therefore, security is a very important issue for this new system, and fine-grained cross-domain security access control and efficient data analysis are the core problems. However, there is still no efficient theory and method to support the research in this area, and some key scientific problems should be resolved. The complexity and randomness from social networks raise difficulties for assessing the security of services and discovering security services accurately and effectively.

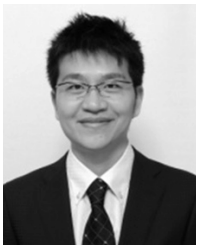
This paper focused on the security of cross-domain data usage control for WSNs in industrial systems. We first established the trust model for Certificate Authority. Then, a login protocol for the user and cross-domain secure authentication protocol were proposed. Next, a fine-grained cross-domain data usage control mechanism is proposed. Based on the above issues, the fuzzy cluster data analysis scheme is provided. The simulation results verify the feasibility of the overhead time and the feasibility and effectiveness of the proposed scheme.

REFERENCES

[1] M. Dong, T. Kimata, K. Sugiura, and K. Zettsu, "Quality-of-experience (QoE) in emerging mobile social networks," *IEICE Trans. Inf. Syst.*, vol. E97-D, no. 10, pp. 2606–2612, Oct. 2014.
[2] J. Wu and S. Shimamoto, "Usage control based security access scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2010, pp. 1–5.
[3] L. Guo, J. Wu, Z. Xia, and J. Li, "Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2577–2586, May 2015.
[4] J. Wu, M. Dong, K. Ota, Z. Zhou, and B. Duan, "Towards fault-tolerant fine-grained data access control for smart grid," *Wireless Pers. Commun.*, vol. 75, no. 3, pp. 1787–1808, 2013.
[5] A. Cassidy, M. Strube, and A. Nehorai, "A framework for exploring social network and personality-based predictors of smart grid diffusion," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1314–1322, May 2015.
[6] Q. Huang, X. Li, J. Zhao, D. Wu, and X.-Y. Li, "Social networking reduces peak power consumption in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1403–1413, May 2015.
[7] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, 2012.
[8] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the Internet of Things," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1193–1195, Nov. 2011.
[9] H. Ning and Z. Wang, "Future Internet of Things architecture: Like mankind neural system or social organization framework?" *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 461–463, Apr. 2011.
[10] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.
[11] M. A. Rahman, A. El Saddik, and W. Gueaieb, "Augmenting context awareness by combining body sensor networks and social networks," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 2, pp. 345–353, Feb. 2011.
[12] M. C. Domingo, "A context-aware service architecture for the integration of body sensor networks and social networks through the IP multimedia subsystem," *IEEE Commun. Mag.*, vol. 49, no. 1, pp. 102–108, Jan. 2011.
[13] *SMART Cities Search Engine*. [Online]. Available: http://www.gla.ac.uk/research/infocus/themes/futurecities/projects/headline_289737_en.html, accessed Sep. 15, 2015.
[14] X. Zhang, F. P. Presicce, and R. Sandhu, "Formal model and policy specification of usage control," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 4, pp. 351–387, Nov. 2005.
[15] S. S. Ray, *Graph Theory With Algorithms and Its Applications: In Applied Science and Technology*. New Delhi, India: Springer, 2013.
[16] O. Wolkenhauer, *Data Engineering: Fuzzy Mathematics in Systems Theory and Data Analysis*. New York, NY, USA: Wiley, 2001.
[17] *NetLogo*. [Online]. Available: http://ccl.northwestern.edu/netlogo/, accessed May 10, 2015.
[18] *OSVDB*. [Online]. Available: http://osvdb.org/, accessed Mar. 2, 2015.
[19] T. D. Nguyen, M. A. Gondree, D. J. Shifflett, J. Khosalim, T. E. Levin, and C. E. Irvine, "A cloud-oriented cross-domain security architecture," in *Proc. Military Commun. Conf. (MILCOM)*, Oct./Nov. 2010, pp. 441–447.
[20] J. Huang and D. Nicol, "Security and provenance in M3GS for cross-domain information sharing," in *Proc. Military Commun. Conf. (MILCOM)*, Oct./Nov. 2012, pp. 1–6.
[21] Y. Yao, X. Wang, and X. Sun, "A cross heterogeneous domain authentication model based on PKI," in *Proc. 4th Int. Symp. Parallel Archit., Algorithms, Program. (PAAP)*, Dec. 2011, pp. 325–329.
[22] X. Zheng, "Cross-domain authentication model in SOA based on enterprise service bus," in *Proc. 2nd Int. Conf. Comput. Eng. Technol. (ICCET)*, Apr. 2010, pp. V5-78–V5-82.
[23] D. Ni, H.-J. Shi, C. Yuan, and J.-H. Guo, "Attribute based access control (ABAC)-based cross-domain access control in service-oriented architecture (SOA)," in *Proc. Int. Conf. Comput. Sci. Service Syst. (CSSS)*, Aug. 2012, pp. 1405–1408.
[24] N. A. Nordbotten, "Cross-domain access control in a military SOA," in *Proc. Military Commun. Conf. (MILCOM)*, Oct./Nov. 2010, pp. 448–455.
[25] S. Eggersgluss and R. Drechsler, "Efficient data structures and methodologies for SAT-based ATPG providing high fault coverage in industrial application," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 30, no. 9, pp. 1411–1415, Sep. 2011.
[26] K. Ahmed, I. Izadi, T. Chen, D. Joe, and T. Burton, "Similarity analysis of industrial alarm flood data," *IEEE Trans. Autom. Sci. Eng.*, vol. 10, no. 2, pp. 452–457, Apr. 2013.



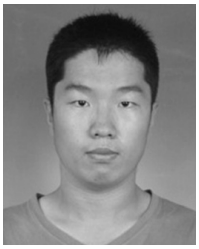
JUN WU received the Ph.D. degree in information and telecommunication studies from Waseda University, Japan. He was a Post-Doctoral Researcher with the Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology, Japan, from 2011 to 2012. He was a Researcher with the Global Information and Telecommunication Institute, Waseda University, from 2011 to 2013. He hosted and participated in several research projects of the National Natural Science Foundation of China, the National 863 Plan, and the National 973 Plan. He is currently an Associate Professor of Electronic Information and Electrical Engineering with Shanghai Jiao Tong University, China. His research interests include advanced computation and communications techniques that involve smart sensors, wireless communication systems, industrial control systems, wireless sensor networks, smart grids, and other related technologies.



MIANXIONG DONG received the B.S., M.S., and Ph.D. degrees in computer science and engineering from The University of Aizu, Japan. He was a Researcher with the National Institute of Information and Communications Technology, Japan. He was a Japan Society for the Promotion of Sciences (JSPS) Research Fellow with the School of Computer Science and Engineering, The University of Aizu, and a Visiting Scholar with the BBCR Group, University of Waterloo, Canada, supported by the JSPS Excellent Young Researcher Overseas Visit Program from 2010 to 2011. He was selected as a Foreigner Research Fellow (a total of three recipients all over Japan) by the NEC C&C Foundation in 2011. He is currently an Assistant Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. His research interests include wireless sensor networks, vehicular ad hoc networks, software-defined networks, big data, and cloud computing. He serves as an Associate Editor of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, the IEEE ACCESS, and *Cyber-Physical Systems* (Taylor & Francis), a Leading Guest Editor of *ACM Transactions on Multimedia Computing, Communications and Applications*, the IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, and *Peer-to-Peer Networking and Applications* (Springer), and a Guest Editor of *IEICE Transactions on Information and Systems*, *Mobile Information Systems*, and *International Journal of Distributed Sensor Networks*. He serves as the Program Chair of the IEEE SmartCity 2015 and the Symposium Chair of the IEEE GLOBECOM 2016. He is a Research Scientist with the A3 Foresight Program (2011–2016) funded by JSPS, the National Natural Science Foundation of China, and the National Research Foundation of Korea.

KAORU OTA received the M.S. degree in computer science from Oklahoma State University, USA, in 2008, and the Ph.D. degree in computer science and engineering from The University of Aizu, Japan, in 2012. From 2010 to 2011, she was a Visiting Scholar with the BBCR Group, University of Waterloo, Canada. She was also a Japan Society of the Promotion of Science (JSPS) Research Fellow with the Kato-Nishiyama Laboratory, Graduate School of Information Sciences, Tohoku University, Japan, from 2012 to 2013. She has been with the JSPS A3 Foresight Program as one of the primary researchers since 2011, which is supported by the Japanese, Chinese, and Korean Government. She is currently an Assistant Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. Her research results have been published in 90 research papers in international journals, conferences, and books. Her research interests include wireless sensor networks, vehicular ad hoc networks, and ubiquitous computing. She was the Best Paper Award Winner of ICA3PP 2014, GPC 2015, and the IEEE DASC 2015. She serves as a Guest Editor of the IEEE WIRELESS COMMUNICATIONS and *IEICE Transactions on Information and Systems* and an Editor of *Peer-to-Peer Networking and Applications* (Springer), *Ad Hoc & Sensor Wireless Networks*, and the *International Journal of Embedded Systems* (Inderscience).

MUHAMMAD TARIQ (M'10) is a Post-Doctoral Fellow with the Department of Electrical Engineering, Princeton University, USA. He is also an Assistant Professor with the Department of Electrical Engineering and the Co-Director of the NUSys Research Laboratory with Fast University Peshawar Campus. He has delivered research talks in FAST-NUCES Islamabad, UET Peshawar, and Umm Al-Qura University, Mecca, Saudi Arabia. He delivered a keynote speech in a seminar on WSN with the University of Peshawar. He is active in wired and wireless communication, control, microgrid design, and automation on the smart grid. He has authored or co-authored 40 research papers, including book chapters, IF journals, and peer-reviewed international and local conferences. He has co-authored a book entitled *Smart Grid Standards: Specifications, Requirements, and Technologies* (John Wiley and Sons, 2015) with leading researchers. His research interests include mathematical modeling, design, and analysis of wireless ad-hoc and sensor networks. He is a member of IEICE, JSST, and PEC. He won the Student Paper Award in the 72nd IEEE VTC 2010 Conference in Ottawa, Canada, and the Outstanding Presentation Award in the JSST 2011 Conference in Tokyo. He also won a Brain Korea 21 Research Grant from the Ministry of IT, Korea, from 2008 to 2009. He is the Editorial Board Member of various peer-reviewed journals and a TPC Member of distinguished conferences.



LONGHUA GUO received the B.S. degree in electronic information engineering from Tianjin University, Tianjin, China, in 2013. He is currently pursuing the Ph.D. degree with Shanghai Jiao Tong University, Shanghai, China. He participates in many national projects, such as the National Natural Science Foundation of China and the National 973 Planning of the Ministry of Science and Technology, China. His research interests include sensor network security and smart grid security.