A Service-oriented Identity Authentication Privacy Protection Method in Cloud Computing

Xiaohui Li[1,3], Jingsha He[1,2] and Ting Zhang[1]

[1]*College of Computer Science and Technology,*
Beijing University of Technology, Beijing 100124, China
E-mail: lixiaohui@emails.bjut.edu.cn
[2]*School of Software Engineering,*
Beijing University of Technology, Beijing 100124, China
[3]*College of Electrical and Information Engineer, Liaoning University of Technology*
Jinzhou, Liaoning, 121001, China

Abstract

Cloud computing provides elastic, scalable on-demand IT services for individuals and organizations. In the cloud computing, everything is as the service. Cloud clients enjoy convenience and efficiency service, but at the same time encounter new issues. Cloud clients needs to provide authentication information to access to service, which often contains a lot of sensitive information. The service provided by Cloud is dynamic, diverse, and context-related. The traditional identity authentication methods which implement coarse-grained to allow or prohibit access is no longer to adapt service-oriented cloud computing. In this paper, we propose a service-oriented identity authentication privacy protection method. In the method, we define cloud service access control as a process and extending the cloud client related information into a fuzzy set as the authentication condition for the exchange, according to the amount of information security level, dynamic opening the corresponding service access control and providing fine-grained service-oriented identity authentication, guarantees global minimal sensitive information disclosure, and maximally protects individual privacy.

Keywords: *identity authentication, cloud computing, service-oriented, fuzzy set, privacy*

1. Introduction

Cloud computing provide the elastic resources on demand, it is form of a collection of services. However, cloud computing brings not only convenience and efficiency, but also security issues, especially data security and privacy protection. In the cloud, cloud servers and clients often located in different security domains and the demand for services with a dynamic, fast, continuous (diversity).Traditional authentication methods based on what you know, which justifies the means, using a static password data or dynamic password technology uses a one-time pad, each time a user logged on through a long list of keyboard input regular password, mismatched performance of popular influence. Traditionally authorization in access control is the act of checking to see if a user has the proper permission to access a particular file or perform a particular action, assuming that user has successfully authenticated himself. Authorization is very much credential focused and dependent on specific rules and access control lists preset by the web application administrator or data owners. Typical authorization checks involve querying for membership in a particular user group, possession of a particular clearance, or looking for that user on a resource's approved access control list,

akin to a bouncer at an exclusive nightclub. Any access control mechanism is clearly dependent on effective and forge-resistant authentication controls used for authorization [1-3].

The traditional identity authentication methods which implement coarse-grained to allow or prohibit access tend to ensure the security service provider, that is no longer to adapt service-oriented cloud computing. Accordingly, researchers introduce trust negotiation into cloud computing access control, through consultation methods, and establish trust relationship chain, thus achieving dynamic resource access control.

Negotiation-based authentication method which establishes trust between strangers through iterative disclosure of digital credentials and access control policies providing enough security guarantees for people who want to share resource across security domains in open systems. But credential, access control strategies usually carry a lot of private information, unlimited disclosure of interoperability is bound to bring many safety hazards and risks in cloud computing of multi-domain environment. To solve this problem, in this paper, we propose a service-oriented identity privacy protection method. In the method, we define identity authentication as a process, and cloud clients expand their own information into the composition class tree structure, according to its security level dynamic and open access of the corresponding service, access to the corresponding service. During transmission extending the authentication information into a fuzzy set, to provide security for the users of cross-domain resource access, provide fine-grained authentication process, at the same time protect the clients' privacy in the cloud.

The rest of this paper is organized as follows. In Section 2, we describe some related work. In Section 3, we explain our service-oriented identity authentication approach for privacy protection in two aspects: one is to relevant definitions and the other is algorithm description. We also give an application scenario for better illustration of our method. In Section 4, we perform some simulations using Opnet in which the results and analysis show that our method can achieve our goal well. Finally, we conclude this paper in Section 5.

2. Related Works

To our knowledge, there is already some identity authentication mechanism to protect privacy.

Personalized search refers to search experiences that are tailored specifically to an individual's interests by incorporating information about the individual beyond specific query provided. Access control filter [4] is a preliminary authorization scheme that checks if the current user can perform the requested controller action. The authorization is based on user's name, user IP address and request types. Access Control Lists are filters that enable you to control which routing updates or packets are permitted or denied in or out of a network. They are specifically used by network administrators to filter traffic and to provide extra security for their networks.

Personalized access control and access filter can be used to choose value information through subjective, but access filter is the way to add a barrier by subject while receiving the results; personalized access control is still to provide the more information, more access to the information service. They are both based on the static information and adopt first access last control mode. In essence, they do not reduce the information disclosure of the vast amounts of information to the user and system. In the cloud computing environment, the cloud terminal is resource-constrained, these methods are not applicable.

Fuzzy sets [5-8] were introduced simultaneously by Lotfi A. Zadeh and Dieter Klauain 1965 as an extension of the classical notion of set. In classical set theory, the

membership of elements in a set is assessed in binary terms according to a bivalent condition — an element either belongs or does not belong to the set. By contrast, fuzzy set theory permits the gradual assessment of the membership of elements in a set [9-11]; this is described with the aid of a membership function valued in the real unit interval [0, 1]. The relevant theory is as follows:

Definition: A fuzzy set is a pair (A,m) where A is a set and m:A[0,1]. For a finite set $A = \{x_1,...,x_n\}$, the fuzzy set (A,m) is often denoted by $\{m(x_1) / x_1,...,m(x_n) / x_n\}$.Then x is called not included in the fuzzy set(A,m)if m(x) = 0, x is called fully included if m(x) = 1, and x is called a fuzzy member if $0 < m(x) < 1$.The set is called the support of (A,m) [12-19].

Equivalence relation: Let R be a binary relation on a set A.

If R satisfies the following conditions: reflexive; symmetry; transitivity; Then R is called an equivalence relation defined on A.Set partitioning: The division of the set X is a nonempty subset of a collection of X, making all elements x of X is the precise subset of one. Equivalent, X a subset of the set P is a division of X, if the elements of P is the empty set; P elements and set equal to X; the intersection of any two elements of P is empty.

3. Service-oriented Authentication Method

In the section, we first introduce the method description and relevant definitions algorithm in detail.

3.1 Method Description

Service-oriented authentication method in the cloud computing triggered by the cloud clients' need , the process as followed:

1) cloud clients information partitioning and extracting to form a hierarchical tree structure;

2) information and services analysis and comparison, using the fuzzy algorithm for tree mapping;

3) processing to complete the certification at the same time determine the mode of service category;

4) using the fuzzy algorithm to complete the secure transmission of user authentication information in the cloud.

3.2 Relevant Definitions

Definition 1: The cloud user information extraction

Extract the semantics of the user information, abstract information attributes and classes, the formation of the hierarchical tree protection strategy, set up a protection strategy for the security level $X = \{X_1, X_2, X_3, ..., X_n\}$ is by $X_i(1 \le i \le m)$ consisting of a collection of Xi is composed of triples by the dense Si and privacy R_i and privacy of the interaction space $X_i = (S_i, R_i, O'_i)$, in which $S_i \subseteq S$, $R_i \subseteq R$, O'_i is a division of space granularity then X is the one with the space constraints and drawing collections, referred to as the security level for the null effect. It represents the granularity of the security level of the same strategy space in the same space.

Definition 2: Service

The service is defined as a monotonic function of f (x) = r the range of 0 to 1, permission from the prohibition to allow. Service abstract for the operation and object encapsulation, it provides users with a call interface. It can be seen from the definition 1, any two elements,

This simplifies the management of access control object, and better adapts to service-oriented computing environment, and access control from the static protection of resources transferred to the authorized service dynamic protection.

Definition 3: tree mapping

T represents the tree. Take the fixed point x belongs to T, val (x) indicates the number of connected components. If val (x) = 1, called point x T is an endpoint; if val (x)> 2, then we call point x is a fulcrum of all the fulcrum of the tree T denoted the closure of each connected component of V (T), the number of T denoted Edg (T). [A] is the smallest closed connected subset of T contains. In particular, for any a, bT, [a, b] represents the measure of the tree. The root node is all the information for the user, more and more detailed information granularity from top to bottom layers of increment, availability of services permissions are getting smaller and smaller and finally close to zero. Figure 1 illustrates service and information structure tree mapping in details.

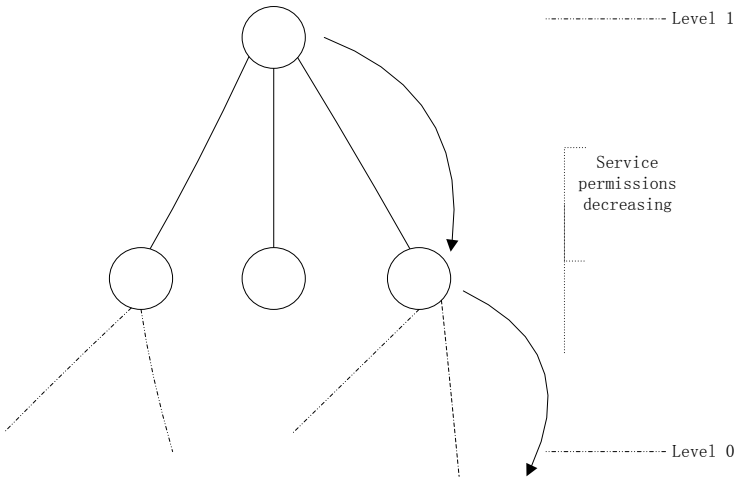

Figure 1. Service and Information Structure Tree Mapping

Define 4: The process of certification

Certification process description, we have done the assumption that, in front of a closed house, the furnishings in the house is the resources required (service), but this door we have only two possibilities: open or close (just as the traditional sense of the access control to allow or prohibit), from another point of view we describe such a process, in order to obtain the items inside the house, opened the door slowly, in other words, we see a little to the items inside the house, until you see all (which is equivalent to the authentication process);

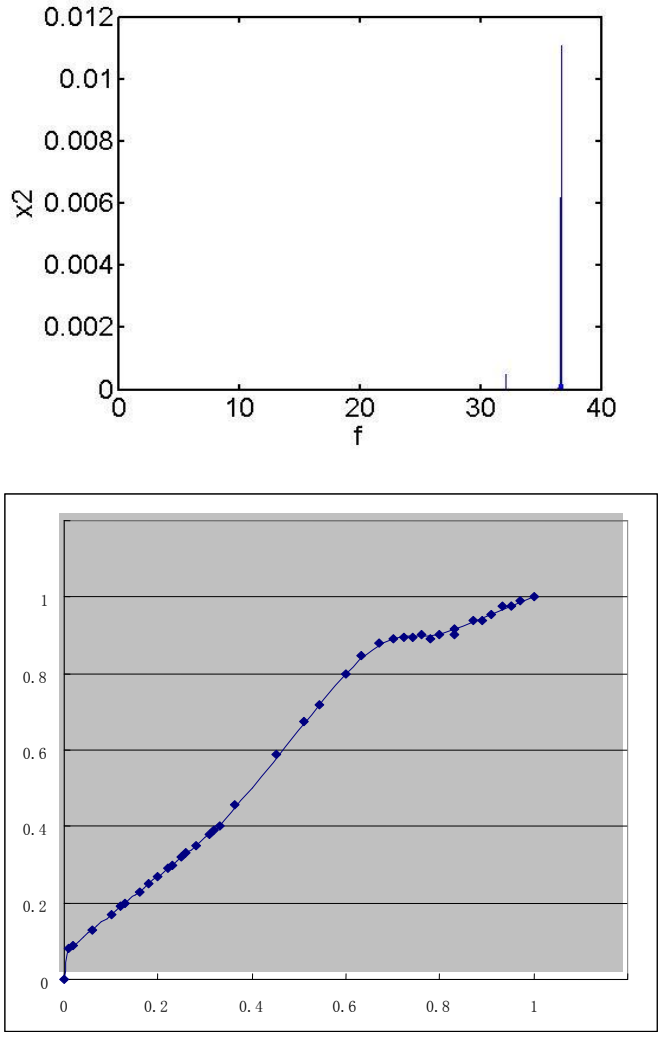

Figure 2. Example of f: [0,1] -> (0,1)

Function f(x)=y, where x is the cloud clients' information protection policy security level, the range [0,1] y is certification process range(0,1) f: [0,1] -> (0,1) ,for example :when i >= 1, $f(2^{(-i)})=2^{(-i-2)}$, Other f (x) = x

In order to satisfy the information service optimization, rules as followed:

Rule1 (granularity control rule): the subject (user) has negative authorization access right to the object (information) of high-level, then subject has the right to all nodes of the object group.

Rule2 (inheritance allowed rule): the subject has the negative authorization access right to the object, default of the principal in the case where the group members of subject have the right to the object;

Rule3 (explicitly deny permission rule): For particular subjects, explicitly deny permission needed.

There are use-cases that involve certain documents, web applications where only negative authorization access shall be granted to very specific users of one or more. In such a case, the users that shall get the right most probably don't share a common attribute that would allow setting rules.

Context. It is any information that can be used to characterize the situation of entities that are considered relevant to the interaction between a user and an application, including the user and the application themselves. Context is typically the location, identity and state of people, groups and computational and physical objects.

Fuzzy set. Let X be the universe of discourse, for any fuzzy set A, the function μ_A represents the membership function [9-10] for which $\mu_A(x)$ indicates the degree of membership that x, of the universal set X, belongs to set A and is, usually expressed as a number between 0 and 1

$\mu_A(x)$: $X \rightarrow [0,1]$; $x \rightarrow \mu_A(x)$

The operation of union, intersection and complementation are defined exactly the same as they are for standard sets in terms of the characteristic function; i.e.:

- Union: $\mu_{A \cup B}(x) = \max(\mu_A(x), \mu_B(x))$
- Intersection: $\mu_{A \cap B}(x) = \min(\mu_A(x), \mu_B(x))$
- Complement: $\mu_{notA}(x) = 1-\mu_A(x)$

The notation for fuzzy sets: For the member of a discrete set with membership μ,we use the notation μ/x .

$A = \mu_1/x_1+\mu_2/x_2+\cdots..+\mu_n/x_n$.

3.3 Algorithm Description

The algorithm consists of the following five steps:

Step1:Cloud server-side S receive the cloud client C service requests sr, According to the information P submitted by C, if sr is an unprotected resource, then immediately grant the access request permission to successful. Otherwise, turn to Step 2.

Step2: S transfer authentication strategy to C request service, the elements in the authentication policy represent the corresponding authentication information of user application service, such as user identity, location information and other sensitive information.

This segment process the context information by four steps.

1. Scan the context information that consists of the users' requirement and context information as the input conditions, Based on user interest categoriesA_1, A_2, ..., A_n. To ensure that A_1, A_2, ..., A_n. independent, there is no intersection.

2. let A be a finite universe U = {X_1, X_2, ..., X_n}fuzzy sets, U is the collection of all information in the cloud server, A is the collection of cloud user information composed byA_1, A_2, ..., A_n. X is the element of U in the cloud server, that is the composition of our cloud user information service set.

According to formula $A = \mu_1/x_1+\mu_2/x_2+\cdots..+\mu_n/x_n$ Where "+" shows a concepts of collection, not the sum of arithmetic. The denominator is the element of domain, molecule is the membership degree of element to A.

3. According to the previous formula, select $\mu_A(x) \leq 0.6$, Choose to meet a fuzzy set A_1 of all x, delete operation. for $A_1 \cap A_2$, ..., $\cap A_n \subseteq \ldots, \subseteq A_1 \cap A_2 \subseteq A_1$,

We have performed evaluation of our method with both sides of the type Gauss membership function using the Matlab simulation software.

Function y = gauss2mf ([x1 x2 ... xn], [sig1 c1 sig2 c2])

For a given domain x and parameters [sig1 c1 sig2 c2], return the corresponding y values for the two-sided Gaussian composite membership function.

4. The information service results include two parts: a public concern (selected according to the read rate); one is the selection results of the third step.

It is designed for the scene of the cloud users acceptance of information services, but can also be applied in other similar occasions. It reflects the psychological needs of the cloud users to information services. When the users want the information provided in the cloud resource pool to obtain the information they most want, we need some specific information of the users, the cloud server make the control and give the results. It is different from the keyword-based search, the results include information that has nothing to do with the specific information of the users.

Step3: According to the authentication information, user information extraction to form a hierarchical tree using fuzzy algorithms and the necessary services to the value of the mapping, steering the request of P layer to determine l（the same layer of information can be used for authentication or not in the information tree）,if l = 1 the specific scenarios to decide whether to disclose the layer information; if l = 0 indicates that disclosure of the conditions are not met, the end;

Step4: Turn to the next level of P to determine the l value, if l = 1 meet the conditions of access, according to specific application scenarios whether disclosure of the layer of privacy information; if l> 0 does not meet the exposed conditions, turn to (5);

Step5: C collate authentication data, authentication information and redundant information written in a collection, extending to fuzzy sets, which is passed to the S with the equivalence relation in a secure transmission.

4. Simulation Results

We have performed evaluation of our method using the Opnet simulator platform and we implemented a simulator written in Visual C++. According to the type of services required the dynamic user authentication information icon. In which the horizontal axis shows the user information, the longitudinal axis shows the fine-grained service access control permissions.

In this paper, our method describes the cloud identifiable information owned by the user (service requester) by the security level tree. Simulation results show that for the same types of services, cloud user authentication information requires to be less than the traditional methods of authentication, and dynamic, able to meet the needs of user privacy protection in the cloud.

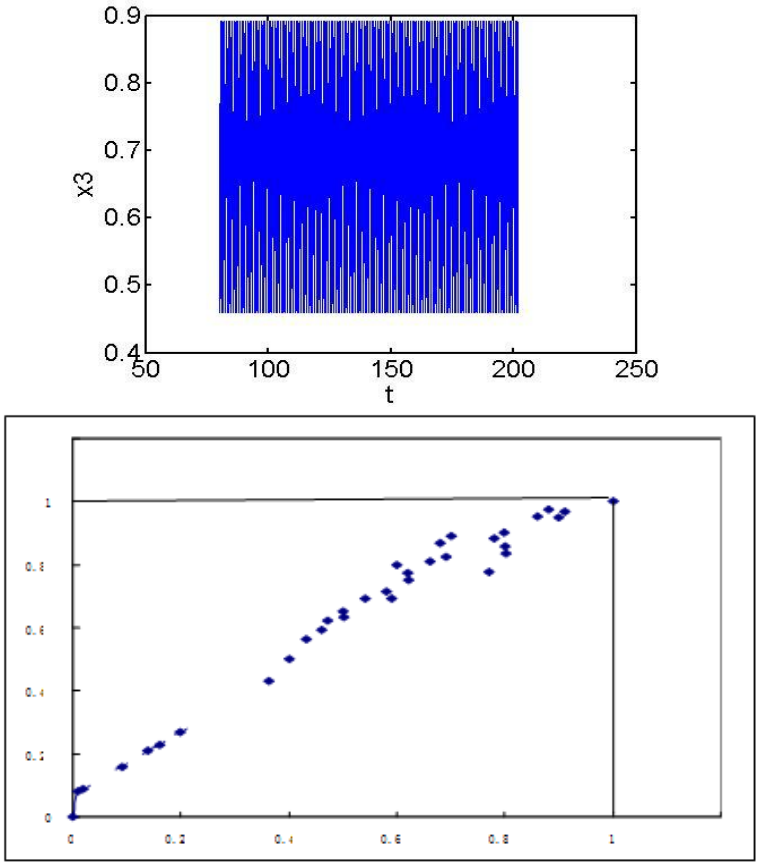

Figure 3. Fine-grained Service Access Control Permission

5. Conclusion

In this paper, we proposed a service-orient authentication method for privacy protection in cloud computing in which we define identity authentication as a dynamic and flexible process that offers a new perspective for authentication. In addition, it can be applied for secure transmission of authentication information. Simulation results show that the performance of our method is obvious and it can help achieve less privacy loss and more fine-grained during exchange of privacy information in the cloud computing.

The method proposed in this paper exposes us to a number of possible research directions in the future. One such direction that we will take is to refine our method to support multi-services. We will also implement the method to study the performance issues and to help us further optimize the method.

References

[1] E. Bertino, P. Samarati and S. Jajodia, "A Temporal Access Control Mechanism for Database System", IEEE Transactions on Knowledge and Data Engineering, vol. 8, no. 1, **(2004)**, pp. 67–80.

[2] E. Bertino and C Bettini, "An access control model supporting periodicity constraints and temporal reasoning", ACM Transactions on Database Systems, vol. 23, no. 3, **(1998)**, pp. 231–285.

[3] M. Curphey, *et al.*, "A Guide to Building Secure Web Applications", The Open Web Application Security Project, Version 1.1, **(2002)**.
[4] S. Haykin, "Adaptive Filter Theory", Fourth Edition, New Jersey: Pearson Hall, **(2002)**.
[5] L. A. Zadeh, "Fuzzy sets", Information and Control, vol. 8, no. 3, **(1965)**, pp. 338–353.
[6] S. Gottwald, "An early approach toward graded identity and graded membership in set theory", Fuzzy Sets and Systems, vol. 161, no. 18, **(2010)**, pp. 2369–2379.
[7] H. Bandemer, "Fuzzy Local Inference in Fuzzy Knowledge Bases", in V. Novak, J. Ramik, M. Mares, M. Cerny and J. Nekola (eds.), Fuzzy Approach to Reasoning and Decision-Making, **(1990)**, Bechyne, Czechoslovakia, pp. 47-48.
[8] L. X. D. Ye, "No division and the set of periods for treemaps", Ergod Th& Dynam Sys., vol. 15, **(1995)**, pp. 221- 237.
[9] M. Khambatti, P. Dasgupta and K. D. Ryu, "A role-based trust model for peer-to-peer communities and dynamic coalitions", In: Proc. of the 2nd IEEE Int'l Information Assurance Workshop. Charlotte: IEEE Computer Society, **(2004)**, pp. 141−154.
[10] X. Li and J. He, "A User-Centric Method for Data Privacy Protection in Cloud Computing", 2011 International Conference on Computer, Electrical, and Systems Sciences and Engineering, **(2011)**, pp. 355-358.
[11] M. A. Moharrum and M. Eltoweissy, "A Study of Static versus Dynamic Keying Schemes in Sensor Networks", Proc. of the 2nd ACM Int'l Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, New York, USA: ACM Press, **(2005)**, pp. 122-129.
[12] L. Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression", International Journal of Uncertainty, Fuzziness and Knowledge Based Systems, vol. 10, no. 5, **(2002)**, pp. 571- 588.
[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel and W. Jonker, "Ciphertext-Policy attribute-based threshold decryption with flexible delegation and revocation of user attributes", Technical Report, Centre for Telematics and Information Technology, University of Twente, **(2009)**.
[14] D. Nurmi, R. Wolski and C. Grzegorczyk, "Eucalyptus: A Technical Report on an Elastic Utility Computing Archietcture Linking Your Programs to Useful Systems", Tech. Rep. 2008-10, University of California, Santa Barbara, **(2008)** October.
[15] C. Castelfranchi, R. Falcone and G. Pezzulo, "Integrating trustfulness and decision using fuzzy cognitive maps", Trust Management 2003, LNCS 2692, **(2003)**, pp. 195-210.
[16] A. Dey, D. Salber and G. Abowd, "A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications", Special issue on Context-Aware Computing in the Human-Computer Interaction (HCI) Journal, vol. 16, no. 2-4, **(2001)**, pp. 97-166.
[17] B. J. Jansen, A. Spink and T. Saracevic, "Real Life, Real Users, and Real Needs: A Study and Analysis of User Queries on the Web", Information Processing and Management, vol. 36, no. 2, **(2000)**, pp. 207-227.
[18] T. Y. M. Winslett and K. Seamons, "Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation", ACM Transactions on In formation and System Security, vol. 6, no. 1, **(2003)**, pp. 1- 42.
[19] P. Bonatti and P. Samarati, "A unified framework for regulating access and information release on the web", Journal of Computer Security, vol. 10, no. 3, **(2002)**, pp. 241- 272.

Authors

Xiaohui Li is currently a Ph.D. candidatein theCollegeofComputer Scienceand Technology at Beijing University of Technology. Her research interests include network security and trust management.

Email: lixiaohui@emails.bjut.edu.cn

Jingsha He is currently a professor of the School of Software Engineering at Beijing University of Technology. His research interests include network security and wireless communication technologies.

Email: jhe@bjut.edu.cn

Ting Zhang is currently a PH.D. candidate in Beijing University of Technology, Her research interests include localization technology and network security in wireless sensor networks.

Email: zhangting06@emails.bjut.edu.cn